大奖
15000美元
挑战智力极限

密码故事

人类智力的另类较量

THE SCIENCE OF SECRECY FROM ANCIENT EGYPT TO QUANTUM CRYPTOGRAPHY

读懂本书，并将所附10道密码按其规则破译，即可获得15000美元巨奖。

〔英〕西蒙·辛格 著

朱小篷　林金钟 译

THE CODE BOOK

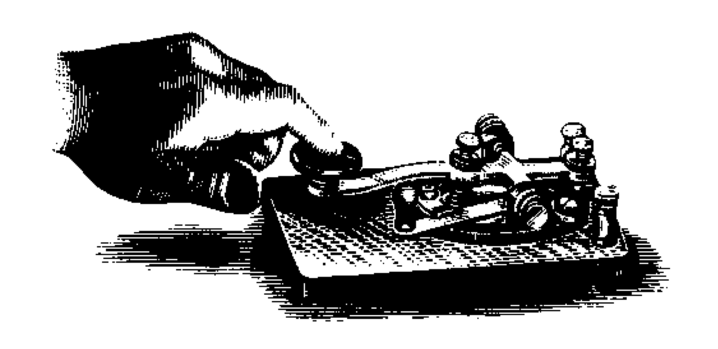


海南出版社

密码故事

人类智力的另类较量

〔英〕西蒙·辛格 著
朱小篷　林金钟 译



海南出版社

图书在版编目(CIP)数据

密码故事/(英)辛格(Singh,S.)著;朱小蓬译.
——海口:海南出版社,2001.9
书名原文:THE CODE BOOK
ISBN 7-5443-0218-0
Ⅰ.密… Ⅱ.①辛… ②朱… Ⅲ.密码-基本知识 Ⅳ.TN918.1
中国版本图书馆 CIP 数据核字(2001)第 062684 号

密码故事

(英)西蒙·辛格 著
朱小蓬 林金钟 译
责任编辑 野夫 莫竹岑
※
海南出版社出版发行
(570216 海口市金盘开发区建设三横路 2 号)
全国新华书店经销
北京市通州运河印刷厂印刷
2001 年 10 月第 1 版 2001 年 10 月第 1 次印刷
开本:850×1168 毫米 1/32 印张:11.75
字数:218 千字
书号:ISBN 7-5443-0218-0/N·1
定价:20.00 元

前　言

几千年来，无论是国王、女王还是将军，在管理国家或指挥军队中一直离不开一个高效的通讯系统。同时他们都明白，假如他们的信息落入对手的手中，也就等于将珍贵的机密泄露给了敌国。至关重要的情报被敌军掌握，那将会导致什么后果？正是由于这种情报可能被敌方截获的威胁推动了密码或代码术的发展：一种伪装信息的技术，使得只有联络好的信息接收者才能够读懂它。

对密码的需求必然推动了国家建立密码编码机构，他们负责发明使用新的密码来保障通讯的安全。同时，敌方密码破解者正试图破解这些密码，窃取信息。密码破解者通常是语言学上的炼丹者，他们能神奇地把一堆无意义的符号魔术般地变成有意义的单词。几个世纪以来，密码编码者和密码破解者之间的斗争事实就形成了密码的历史。这是一场智力上的接力赛，并且对历史的发展方向往往有着戏剧性的影响。

写这本书有两个主要的目的：第一是讲述密码的演化过程。用演化这个词是恰到好处的，因为密码的发展可以被看成一种演化竞争。一个密码产生之后，便会经常遭受密码破解者的攻击。当密码破解者发展了一种新的武器能够揭示这个密码的弱点，那么这个密码就不再有用。它或者永远消失或者进化为一种更新更

强的密码。同样这个新密码也只能存活到密码破解者发现它的弱点为止,就这样发展下去。这与生物上的抗逆性相似。例如对于一株感染菌,这种细菌先在人体里繁衍生殖,但是一旦医生发现了某种针对它弱点的抗生素,它就无法遁形。这种细菌不得不演化直到能够抵抗抗生素为止。如果成功,它将又一次存活下去,也就是这样,细菌在抗生素的一轮轮攻击下不断地演化。

在密码编码者和密码破译者之间硝烟不断的战争中,一系列令人称谓的科学突破也应之而生。密码编码者一直努力构建一种至强的密码来保障通讯安全,而密码破解者则一直努力发明更有效的方法来攻击它们。在他们解密和保密的斗争中,双方都吸收了各种原理和技术,从数学到语言学,从信息论到量子论,范围很广。反过来,密码编码者和密码破解者又丰富了这些理论,他们的工作促进了技术发展,最值一提的是现代计算机的发明。

历史的道路上到处点缀着密码的踪迹。他们决定着战争的结果,甚至带给国王和女王毁灭性的后果。因此,我完全可以根据某些政治谋略的故事以及生与死的传说,来描述密码演化发展中的一些转折点。然而,密码的历史是丰富的,所以我不得不略过许多迷人的故事,这也表示我的说明不是完全的。对于你所喜爱的故事或你喜欢的密码破解者,如果你想了解得更多你可查阅相关读物,它能帮助一些读者更加详细地了解密码学。

在讨论完密码的演化以及它对历史的影响后,这本书的第二个目的是说明在今天密码是怎样的比以前更加重要。随着信息变成不断增值的商品,加上通讯革命改变着这个社会,给信息加密的过程在日常生活中将扮演一个越来越重要的角色。如今我们的电话要通过卫星,我们的电子邮件要通过不同的电脑,这两种通讯形式都很容易被拦截,这样就暴露了我们的隐私。同样的,随着越来越多的企业通过互联网运作,为了保护公司和他们的客户,防卫措施必须要放在重要的位置。加密是保护我们隐私和保证数字市场

成功的惟一方法。秘密通讯的技术或者叫密码编码术为信息时代提供了锁和钥匙。

10 年来,警察和情报部门使用无线监听来搜集对付恐怖分子和犯罪集团的证据,但是近来密码术的发展直接影响到无线监听的效果。随着人类进入 21 世纪,人们急需密码编码的广泛使用来保护个人隐私。有同样要求的是商业公司,他们需要强大的密码编码术使得他们能在互联网时代保证业务的安全。可是同时一系列政策法规却限制密码编码术的使用。问题在于哪一个更重要——我们的隐私还是有效的政权? 或者有没有一个折中的办法。

现在密码编码术对人类的活动有着巨大的影响,尤其值得一提的是军事密码编码术具有举足轻重的地位。有人说第一次世界大战是化学家的战争,因为芥子气和氯气第一次被用来作为战争武器;第二次世界大战是物理学家的战争,因为原子弹被派上了战场。同样我们可以说,如果有第三次世界大战的话,那将是数学家的战争,因为数学家将控制战争中下一个重要的武器——信息。现在由数学家负责发明新密码来保护军事信息。相应的,数学家也会站在破解这些密码的前沿。

在讲述密码的演化和对历史的影响时,我偏离了一下话题。在第五章我描述几种不同的古代文章的破译,包括 B 类楔形文字和埃及象形文。技术上,密码是与通讯相关,有意设计来保护己方的秘密,而古文明留下的笔迹并不是想用来保密的,问题仅仅是我们不能够解释它。然而复原远古文章内容的技术与密码破解术是非常相近的。约翰·查德威克曾写过一本书,描述了如何揭示一篇古地中海文章的原意。我对那些破译我们祖先留下的文字的人们所取得的智力成就感到震惊,他们使我们知道了我们祖先的文明、宗教和日常生活。

迫于需要,我在书中介绍了密码编码学中多种技术词汇。虽然我一般是按照它们的定义,但难免有时候我会使用一个技术上

并不准确的词汇，这也许对非专业人员来说更加容易接受。

在结束引言之前，我必须提及一个问题，这是每一个密码学方面的作家都要面对的，那就是加密科学很大程度上是一门秘密的科学。书中提到的许多英雄在他们的一生中都没有因他们的工作而得到认可，因为当他们的发明仍具有外交和军事价值时，他们的贡献是不能公开赞颂的。在本书完成过程中，我有幸与英国通讯总部(GCHQ)的专家进行了交谈，他们向我揭示了70年代研究过程的详细细节，这些现在已解密了。其结果是，世界上三位最伟大的密码编码师现在能够得到他们应有的荣誉。然而，这次披露却使我认识到还有许多我以及其他科学作家所不知的事情在进行。像英国通讯总部和美国国家安全局这样的组织在继续进行密码编码的研究，这意味着他们的突破仍需保密，他们本人也只能默默无闻。

尽管涉及到政府机密，我还是用本书最后一章来讨论密码的未来。这一章将试图发现我们是否能够预测在密码编码者和密码破解者之间革命性的斗争中谁胜谁负。密码编码者能够设计出一种真正无法破解的密码，成功满足他们绝对安全的需要吗？或者密码破解者能建造一台能够解密任何信息的机器吗？由于我们知道一些最伟大的头脑仍在秘密实验室工作，他们有足够的科研资金，因此我在最后一章的某些论断显然可能是不准确的。例如我提到虽然量子计算机具有破解今天所有密码的潜在可能，它应该还处在非常原始的阶段，但是可能已有人建造了一台。惟一可以指出我错误的人甚至没有理由来暴露自己的身份。

内容简介

自从人类开始会用笔书写，他们就开始用密码通讯了。密码并不仅仅与电报、军事或爱情相关，它已进入人类生活的很多层面：信用卡、保险柜、电脑等等。密码无处不在，同时又随时可能被破译。围绕密码所展开的斗争甚至远胜于战争本身，它既是人类智力的另类较量，又是数学的神秘之美的比拼。在《密码故事》中，西蒙·辛格讲述了关于间谍、阴谋和聪明才智的精彩故事，从而揭示了密码学引人入胜的历史。

作者的叙述结合了可读性与耐人寻味的专业分析，十分新颖独特。



作者简介

西蒙·辛格在剑桥大学得到了物理学博士学位，曾在BBC做制片人。执导的纪录片《费马大定理》荣获了BAFTA（英国电影和电视艺术学院）大奖。同时他撰写了与纪录片同名的畅销书。

责任编辑：野　夫
　　　　　莫竹芩

选题策划：任建成

封面设计：水　平

目　录

第一章 玛丽女王的密码

1586年8月15日，星期六的早晨，玛丽女王被带到福斯灵海城堡的法庭上，那里已坐满了人。虽然几年的监狱生活加上风湿病的困扰已使她身心憔悴，但她仍保持着一份威严和镇定，显出不容置疑的皇家风范。在随身医师的陪同下，她沿着又长又窄的议室，经过法官、官员和观众席，来到正中的王座前。玛丽试图把王座想像成以一种尊敬的姿态对着她，但她却错了。这个空着的王位就象征着她的敌人而且是检举人——伊丽莎白女王。玛丽轻轻地走过王座，走向屋子的另一边——被告席：一个深红色的绒毛椅子。

苏格兰玛丽女王正因叛国罪被接受审判。她被指控密谋刺杀伊丽莎白女王并取而代之成为英国新女王。伊丽莎白的首席大臣弗朗西丝·沃尔辛厄姆已经逮捕了其他同谋者，逼供并处决了他们。现在，他正设法想证明玛丽是这次计划的核心人物，因而同样有罪，同样该受死刑。

沃尔辛厄姆知道在他能够处决玛丽之前，他必需使伊丽莎白女王信服玛丽确实有罪。虽然伊丽莎白鄙视玛丽，但她也有众多原因不愿看到玛丽被处以极刑。首先，玛丽是苏格兰的女王，许多人怀疑英国法庭是否有权处决一个国外政权的首领？其次，处决



图 1:苏格兰的玛丽女王

了玛丽或许就形成一个使其不安的先例。如果本国政权有权杀死一个女王,那么叛军就会没有什么保留地杀死另一个女王,这可能就是伊丽莎白。再说,伊丽莎白和玛丽本是表亲,她们的血缘关系更加使得伊丽莎白难以定她死罪。一句话,只有沃尔辛厄姆能够

彻底地证明玛丽曾是刺杀计划中的一份子，伊丽莎白才能认同玛丽的死刑。

同谋者是一群年轻的贵族天主教徒，他们志在废黜新教徒伊丽莎白，而让同样是天主教徒的玛丽取代她。其实在法庭上已很明显地表露出玛丽是这些同谋者的幕后主使人，但玛丽是否真正批准过这个谋划却无从得知。事实上，玛丽确实签署过这个计划。摆在沃尔辛厄姆面前的一个挑战就是证明玛丽和其策划者之间这种触手可及的联系。

在她被审判的这天早上，玛丽身穿色调悲哀的黑色丝绒衣，独自一人坐在被告席上。对于叛国罪，被告人不允许有辩护律师，也不允许传叫证人。而对玛丽，甚至不允许其部下帮助她一同准备该案件。然而她的处境也不是毫无希望，因为她曾经也留有一手，就是确保每次和同谋者之间的通信都是用密码写成。密码把她的话变成看似没意义的一系列符号。玛丽相信即使沃尔辛厄姆拿到这些信，他也只能对信中字母的意思感到毫无头绪。如果信中的内容成为一个谜，那么这些信就不能作为对其不利的证据。然而，所有这些都建立在一个假定之上，就是这些密码不能被破解。

不幸的是，沃尔辛厄姆不仅仅是位首席大臣，他还是英国的间谍首脑。他已经截获了玛丽给策划者写的信。他也非常清楚谁能够解开这些密码。汤姆斯·菲利普斯是该国一流的密码破译专家。几年来，他一直在破解那些密谋推翻伊丽莎白女王的贵族之间传递的信息，从而为指控他们提供所需的证据。如果他能解开玛丽和共谋者之间的信，那么她的死刑将是不可避免的。而另一方面，如果玛丽的密码足够安全而掩盖了她的秘密，那么她或许还有一线生机。一条密码即决定着生死存亡，这在历史上已不是第一次。

密文的演化

最早对密文作出一些说明的人可追溯到希罗多德，罗马著名的政治家和哲学家西塞罗称他为“历史之父”，希罗多德以编年史的形式记载了公元前五世纪希腊和波斯之间的冲突，并认为这些冲突是自由和奴役之间的对抗，是保卫独立的希腊国和压迫统治他们的波斯人之间的对抗。根据希罗多德的记载，正是由一种叫密文的技术才使希腊免遭被波斯暴君也是王中之王薛西斯一世征服的厄运。

薛西斯开始选择在波斯波利斯上建一座城堡作为其王国的新首都，不久以后，希腊和波斯之间长期的矛盾达到了顶点。当时，波斯帝国上下及其众多邻国都送来了贡品和礼物，但雅典和斯巴达却一概不献。于是薛西斯决定要报复希腊对他的傲慢，开始调动了一支军队，声称“我们要把波斯的领土扩大到天界，那么在我们自己的领土上空就永远会悬挂着太阳”。他花了五年的时间秘密组成了一支有史以来最强大的军队，到了公元前 480 年，他已经做好了准备，发动一场出其不意的进攻。

然而，波斯的军备建设都被一个名叫德马拉图斯的希腊人看在眼里。这位希腊人曾经被他的祖国驱逐出境，现在住在波斯的苏萨。但尽管已被流放，他仍然对希腊保持着一份忠诚，因此他决定给斯巴达带去消息以告诫他们薛西斯的侵犯企图。可问题是怎样才能够送出信息而不被波斯士兵截住？希罗多德写道：

> 因为被发现后危险会很大，因而只有一种方法他能尝试送出这条信息：就是利用已上蜡的一副可折叠的刻写板，先将蜡刮去，再将薛西斯的阴谋刻写在木板的背

面，然后再涂上蜡盖住消息。这样刻写板看上去没写任何字，一路上就不会被士兵怀疑。当这条信息到达目的地后，没有人能够猜出其中的秘密，就我所知，是克莱奥梅尼的女儿戈尔戈，也就是齐奥达斯的妻子，占卦并告诉其他人如果他们把蜡刮去，他们就会发现在木板的背面写有东西。有人这么做了，于是这条信息被揭开，而后传到其他希腊人手中。

由于得到了警告，一直没有防备的希腊人开始武装自己。以前国家银矿的收入通常被民众分享了，现在转给了海军用来建造了二百艘战船。

薛西斯已经失去了战争的一个关键因素——趁人不备。公元前 480 年 9 月 23 日，当波斯舰队向雅典附近的萨拉米斯海湾开进时，希腊人已经恭候多时了。虽然薛西斯相信他已经包围了希腊海军，但是希腊人正是有意地诱使波斯船队进入海湾。希腊人知道他们的舰船又小又少，在开放海域很易被摧毁。但在海湾领域内，他们却可以运用策略打败波斯。随着风向的改变，波斯人发现他们正被风吹进海湾，钻进了希腊人的陷阱。领军出战的波斯公主三面被围，意图退回到海域。却仅有她自己冲了出来。接着，波斯军大乱，更多的船只撞在一起，希腊人发起了全面猛攻。仅一天，强大的波斯军队被挫败了。

德马拉图斯的这种秘密通讯的策略就在于简单地将信息隐藏起来。希罗多德也讲了另一个例子，在这个例子里信息的隐藏程度足以保证其安全传送。他以年事记的形式讲述了希斯塔亚乌斯的故事：希斯塔亚乌斯想鼓励米勒图斯的阿里斯塔哥拉斯反叛波斯国王，为了秘密地传达他的指示，希斯塔亚乌斯剃光了他的一个信使的头发，将信息写在其头皮上，再等信使的头发重新长起来，很明显这段历史时期发生的还不是什么紧急事件。这个信使显然

不用携带任何异物,能够自由穿行,不会有麻烦。一旦到达目的地,他就剃光头发,指给联络人看。

通过把信息隐藏起来的这种秘密通信称为 Staganography(隐文术),由希腊词 Steganos(意为“覆盖”)和 Graphein(意为“写”)派生而来。从希罗多德以后 2000 多年,各种形式的隐文术被使用。例如,中国古代将信息写在小块丝绸上,塞进一个小球里,再用蜡给封上,然后让信使吞下这个蜡球。16 世纪,意大利科学家乔瓦尼·波塔描述了如何将信息埋藏在一个煮熟的鸡蛋里:他把少许明矾和一点醋混在一起制成一种墨水,再用这种墨水将信息写在鸡蛋壳表面。墨水溶液就会经蛋壳上的微孔渗透进去,在已凝固的鸡蛋白表面留下印迹,这样只能剥去蛋壳后才能读取。隐文术也包括用隐形墨水来写信息,早在公元一世纪普林尼就解释了体液如何用作隐形墨水。用这种液体写的字干后即变得透明,但轻轻地加热就能把液体烤焦,从而字迹就以棕色显现出来。许多有机流体都有这样的性质,因为它们富含碳因而很易被烤焦。事实上,即使是现代间谍也很少知道在标准配备的隐形墨水用完之后还可以用自己的尿来临时代替。

隐文术的长久使用表明它确实起到了一定保密作用,但它也有一个根本的弱点。如果信使被搜查,信息被发现,那么秘密通信的内容也立即暴露无遗。一旦信息被截获,所有的安全性也就随之荡然无存。一个严格的士兵会例行地搜查每一个过境人,包括刮一刮所有上蜡的刻写板,给所有空白纸张加加热,剥开煮熟的鸡蛋,剃光人们的头等等。难免会有发现隐藏信息的时刻。

因此,在隐文术发展的同时,还有另一种方法也在演化,那就是 Cryprography(密码术),从希腊词 Kryptos(意为隐藏)派生而来。密码术的目的不是隐藏信息本身,而是要隐藏它的意思,也就是一种加密的过程。为了使信息无法被外人理解,将信息按照事先在发送者和接收者之间规定好的某种特别规则打乱。那么接收

者可以将打乱的信息恢复原样,信息就可以被理解。密码术的优势在于即使敌人截住了一条加密的信息,也无法读懂它。不知道扰乱的规则,敌方将很难(也并非不可能)重现密文的原始含义。

虽然隐文术和密码术是各自独立的,但完全可以将一条信息既混乱又隐藏以取得一个最安全的效果。例如,二战期间流行的微粒照片是一种隐文术。德军在拉丁美洲的间谍将一页文件缩小在直径不到1毫米的微型照片上,看上去就是一个点,再将这个点状照片贴在看似无关紧要的一封信中的某个句号上面。这种微型照片在1941年第一次被美国联邦调查局发现,紧接着美军就有所警觉,查看信中有无微弱的光点,它可能就是光滑的胶片反射出来的光。从那以后,美军能读懂大多数被截住的微型照片的内容,除非德军间谍有所防范,在缩小之前,将照片中的信息混乱。这样,密码术融进了隐文术中,美军即使有时截获住了通信,但却无法获得关于德间谍活动的任何新的信息。在秘密通讯的上述两种分支中,密码术是更加有效的,因为它能防止确切的信息落到敌军手中。

同样,密码术也被分为两种,即易位和替换。在易位中,组成信息的字母被简单地重排,形成互相颠倒的一组字母序列(我们暂称之为易位句)。对于特别短的信息,例如一个单词,这种方法相对不可靠,因为只有有限的几种方法来重组这几个字母。以三个字母 C O W 为例,仅有六种结果:C O W ,O C W ,C W O ,O W C,W C O ,W O C 。然而,随着字母逐渐增多,重组的可能结果也急剧膨胀,从而不可能再复原到原来的信息,除非知道具体混乱的规则。例如有下面一条信息:For example, consider this short sentence(例如考虑这个短句子)。其中只含有35个字母,然而却有5×10^{31}种不同的排列结果。如果一人每秒能检查一条,世界上所有的人日夜工作的话,那么宇宙泯灭轮回1000次,才能查完所有这些结果。

即使是很短的信息,敌方拦截员要复原出其原意也是不切实际的,因而,字母的随机排列似乎提供了一种很高的安全性。但也有个缺点。易位虽然有效地形成一个极其难的易位句,但是,如果字母既不是按照某种韵律也不是按照其他什么逻辑而是随机地被混乱,那么复原一个易位句对于一个联络好的接收人或对于一个敌方拦截员一样是不可能的。为了使易位行之有效,字母的排列需要遵循一种直接的规律,当然这种规律事先只有发送信息的人和接收人共同知道,并对敌方是保密的。例如,在学校里,学生有时用一种叫"栅栏"的易位方法来传递信息,信息中的字母被交替地写成上下两行,再将下面一行文字附加在上面一行的后面,从而形成一段加密后的信息。例如:

THY SECRET IS THY PRISONER; IF THOU LET IT GO, THOU ART A PRISONER TO IT

↓

T Y E R T S H P I O E I T O L T T O H U R A R S N R O T
 H S C E I T Y R S N R F H U E I G T O A T P I O E T I

↓

TYERTSHPIOEITOLTTOHURARSNROTHSCEITYRSNRFHUEIGTOATPIOETI



图 2:当把皮带从发送人的密码器(木棍)上解下来后,皮带上只显现一些无规则的混乱字母:S、T、S、F……只有当它被绕在另一根直径和发送者所使用木棍一般大的木棍上时,信息才能复原。

接收者只需简单地将上述过程反过来即得到信息。已有许多程序化的易位方法,包括三线栅栏密码,它是先将信息写成三行字

母而不是两行,也可以选择再交换每一对字母,使第一和第二字母交换位置,第三和第四交换位置,依次类推。

另一种易位形式第一次被做成了军用密码装置,那是斯巴达的一种装置,早在公元前五世纪就出现了。这种外观是一根棱形木棍,外面缠绕着一条皮革或羊皮纸(图 2)。发送人先沿着木棍纵向在条带上写上信息,然后再解开条带,那么从条带上就看到一些无意义的字母,信息已被混乱了,信使就可以带着这条皮带,如果再来点隐文术的手段,他可以将其伪装成腰带系在身上,而信息却写在反面。复原信息时,接收者只需简单地把条带绕在一根木棍上,其直径应和发送者使用的一般大。公元前 404 年,斯巴达的莱桑德接见了一位满身血污、憔悴不堪的信使,他从波斯来,本来是五个人,现在只有他在艰难的旅途中存活下来。这位信使把他的皮带递给莱桑德,莱桑德将皮带绕在密码装置上,得知波斯法拿巴兹正计划进攻斯巴达。正是因为这个密码装置,莱桑德才有所准备,并进行了有力还击。

与易位并列的密码术是替换。关于替换加密的最早描述出现在《爱经》中,这是由婆罗门学者写于公元四世纪的一篇文章,但根据手迹来看,可追溯到公元前四世纪。《爱经》建议女人应学会 64 种技术,如做饭、穿衣、按摩和制备香水,还包括一些如咒术、象棋、装订和木工之类的不太常见的技术。第 45 种是密文术。其中介绍的一种方法就是先随机地将字母两两配对,然后将原始信息中的每一个字母用它的配对者来代替。以罗马字母为例,我们可以进行如下配对:

A	D	H	I	K	M	O	R	S	U	W	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
V	X	B	G	J	C	Q	L	N	E	F	P	T

那么,对于句子:meet at midnight (晚上见),发送者将写成:

CU UZ VZ CGXSGIBZ。这种形式的密文叫做替换密码,因为原文中的每一个字母都被换成一个不同字母,所以可以作为易位的一种辅助方法。在易位中字母不变,位置改变;替换中字母改变,位置不变。

将替换密码用于军事用途的第一个文件记载是恺撒著的《高卢记》。恺撒描述了他如何将密信送到正处在被围困、濒临投降的西塞罗。其中罗马字母被替换成希腊字母使得敌人根本无法看懂信息。关于这次奇妙的传送,恺撒是这样写的:

> 信使受到指示,如果他不能接近被围困的军营,他就将信件绑在一根矛上,然后将矛投到被围困的军营内。
>
> 可是掷出的矛碰巧插进一个防塔里,连接两天没有被人发现,第三天一个士兵看见了,取下来交给西塞罗。西塞罗看完之后在全军面前复述了这个信息,大家都倍受鼓舞。

恺撒频繁地使用密文,对此瓦莱利厄斯·普罗布斯做过详细地描述,但不幸失传了。然而有幸的是苏托尼厄斯在公元二世纪写下《恺撒传》,书中对恺撒用过的其中一种替换密码作了详细的描写。恺撒只是简单地将信息中的每一个字母用字母表中的该字母后第三个字母代替。密码学家通常将用来书写原始信息的有关字母称为明码字母表,这里简称明码表;而把用来替换明码字母的有关字母称为密码字母表,这里简称密码表。当把明码表放在密码表的上面时(图 3),很明显密码字母表和明码字母表相比后移了 3 个位置。因而这种形式的替换通常叫做恺撒移位密码,或简单说,恺撒密码。这里我们可以给密码下一个定义:**一个密码是指任何形式的一种隐秘的替换,其中每个字母都被另一个字母或符号代替。**

明码表 a b c d e f g h i j k l m n o p q r s t u v w x y z
密码表 D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

明　文 v e n i, v i d i, v i c i
密　文 Y H Q L, Y L G L, Y L F L

图 3:恺撒密码适用于短消息。恺撒密码字母表只是将明码字母表中字母依次后移(后移 3 位)。在密码学里,通常把明码字母表写成小写体,而密码字母表则写成大写字母。同样,原信息的明文以小写体书写,而加密的信息则用大写。

尽管苏托尼厄斯仅提到三个位置的恺撒移位,但显然从 1 到 25 个位置的移位我们都可以使用,从而对每个字母我们都能构建 25 种不同的密码字母来代替它。实际上,如果我们对移位不加限制,即允许密码字母表是明码字母表的任一种重排,那么我们能得到更大数目的密码字母表。有超过 4×10^{27}种这样的重组,因而存在有同样数目的密码字母表。

每个不同的密码都代表着一种加密方法,包括算法和密钥两元素,这两个元素描述了每种加密的精确细节。在上述例子中,将信息中每个明码字母用密码字母来代替就代表一种算法,而密码字母表可以是明码字母表的任一种重排。密钥则明确了某特定加密过程中所用的密码字母表。关于算法与密钥的关系见图 4。

一个敌人在研究一段被截获的信息时,或许能猜到其所用的算法,却无法得知其所用的特定密钥。例如,他们可能深深地怀疑原始文件中的每一个字母都根据某种密码表被另一个不同的字母代替,但他们不可能知道哪个密码表被使用了。假如密码表,即密钥,只是发送者和接收者之间严守的一个秘密,那么敌人就不能对截住的信息进行解密。和算法相对立,密钥的重要性是密码术中永久的一项原则。对此,1883 年,荷兰语言学家奥古斯特在其所著《密码学》一书中作了权威性的陈述:一个密码系统的安全性不

在于对加密算法进行保密,而仅在于对密钥的保密。

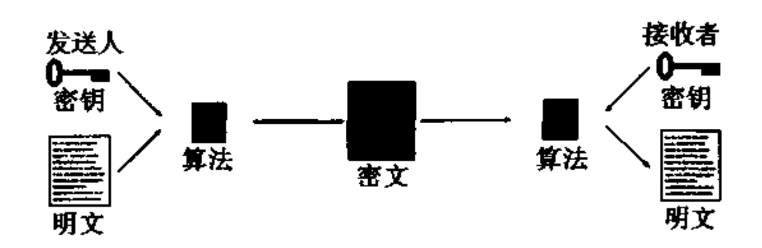


图 4:发送人通过一种加密的算法来加密明文。算法是最普遍的加密系统,并要选择一种特定的密钥同时提供密钥和算法就会使密文解密。在密文送到接收者手中的途中可能会被敌人拦截,所以应防止敌人解密。而接收者既知道算法又知道发送人的密钥,所以密文能被接收者最终解密。

除了对密钥保密外,一个安全的密码系统也必需有一个大范围的可供选择的密钥。例如,如果发送者用恺撒转移密码来加密一段信息,那么这种加密相对就较弱,因为只有 25 种可能的密钥。从敌人来说,如果他们截住了这信息并怀疑其使用的是恺撒移位算法,那么他们只需简单地检查这 25 种可能性即可破解。然而,如果发送者使用更为综合的替换算法,也就是允许密码表是明码表的任一种随意排列,那么就有 4×10^{27}种可能的密钥供选择。图 5 是其中可能的一种。对于敌人,如果信息被截获了,算法也知道了,那么检查所有可能的密钥将是一件可怕的任务。如果一个敌方间谍每秒能检验这 4×10^{27}种可能密钥中的一条,检查完所有这些密钥并破解了信息将花费宇宙轮回 10 亿次所经历的时间。

这种密码很实用,因为它在很容易实施的同时提供了很高的安全性。发送者很容易定义一个密钥,只需说明一下重排后得到的密码表中二十六个字母的顺序,就有效地防止敌人通过所谓蛮力筛选的方法检验所有可能的密钥,密钥的简单性是重要的,因为密钥是

发送者和接收者所共知的，密钥越简单，误解的机会就越小。

明码表 a b c d e f g h i j k l m n o p q r s t u v w x y z
密码表 J L P A W I Q B C T R Z Y D S K E G F X H U O N V M

明 文 et tu, brute?
密 文 WX XH, LGHXW?

图 5：在一般的替换算法例子中，明文中的每一个字母都根据密钥被替换为另一个字母。密钥可被定义为明码字母表的任何一种重新排序的密码字母表。

事实上，如果发送者可以接受密钥数目的稍微减少，密钥甚至可以更简单。发送者可以不通过随机地重排明码字母表来得到密码表，而是选择一个关键词或关键词组。例如，用 JULIUS CAESAR 作为一个关键词组，先将其中的空格和重复字母去掉(JULISCAER)，然后将其作为密码表的前部分密码字母，至于后部分，先将明码字母表中在关键词组中出现过的字母去掉，再按顺序接在其后。因而，所得密码表就是：

明码表 a b c d e f g h i j k l m n o p q r s t u v w x y z
密码表 J U L I S C A E R T V W X Y Z B D F G H K M N O P Q

用这种方法建立一个密码表的优点在于关键词或关键词组容易被记住，因而密码表也一样。这一点很重要，因为如果发送者将密码表写在一张纸上，敌人可能会截获这张纸，从而发现密钥并能读取用该密钥加密的通信。但是，如果密钥仅存留在记忆中，就不太可能落入敌方手中。显然用关键词组产生的密码表数目比那种明码表随机排列产生的数目少得多，但也很大，对敌人也是不可能通过测试所有可能关键词来复原截获的信息。

替换密码的简单有效使其在公元前一个千年里在密文技术领域占尽了优势。密码编码者已经建成了一个系统能够保证安全的通讯,因此如果没有必要,就不必进一步发展,也就无需更深入研究。因而任务就落在了密码破解者的身上,他们要不断地尝试破解替换密码。究竟有没有方法能使敌方拦截者复原一段被加密的信息呢?许多古代学者认为替换密码是无法破解的,庞大数目的可能密钥的存在,使得几个世纪来都被认为是可靠的。但是,密码破解者最终发现了一种捷径来穷搜所有可能的密钥。不用花费数亿年的时间来破解一个密码,通过捷径复原一条信息也就是几分钟的事情。这项突破首先发生在东方,是一次语言学、统计学和宗教信仰之间的卓越的联合。

阿拉伯密码破译师

穆罕默德在大约 40 岁的时候,开始定期光临麦加城外希拉山上与世隔绝的一个山洞,这是一个供人祈祷、冥想和沉思的静修地方。穆罕默德经过一段时间的深思,大约公元前 610 年,天使降临到他面前,并宣称他将是上帝的信使。这是启示录系列中的最初部分,启示录一直保持到约二十年后穆罕默德去世,并在其一生中被不同的抄写家记录下来,但仅是一些片断。他传到了伊斯兰教第一任哈里发(伊斯兰教执掌政教大权的领袖的称号)阿布 - 贝克尔的手中,开始将其整理成文。这项工作由第二任哈里发乌马及他的女儿哈夫萨继续下去,最终由第三任哈里发乌斯曼完工。各个启示录组成了可兰经的 114 个篇章。

在位哈里发负责传递穆罕默德的功绩,高举他的教义,传播他的思想。从 632 年阿布 - 贝克尔成为哈里发到 661 年第四任哈里发阿里去世,伊斯兰教不断传播,以至当时所能知道的世界的一半

都在穆斯林的统治之下。到了 750 年，经过一个世纪的巩固，阿巴斯王朝的建立预示着伊斯兰教文明黄金时期的来临。艺术和科学得到同样程度的繁荣。伊斯兰工匠留给了我们绚丽的绘画，华美的雕刻和有史以来最精致的纺织品。而伊斯兰科学家们的遗产则体现在现代科学词典中数量众多的阿拉伯词汇上，如 algebra（代数学），alkaline（碱）和 zenith（轨道）。

伊斯兰文化的昌盛很大程度上是因为当时社会的富裕与和平。阿巴斯时代的哈里发们同他们的先任者相比不再对征服抱有太大兴趣，相反，他们把精力集中在建立一个有秩序的富裕的社会上。低税收刺激了贸易的增长，形成更庞大的工商业，同时严格的法律减少了腐败并保护了人民。这一切都依赖于一个有效的管理体制，而管理者则依赖于由加密获得的安全的通讯。除了对政府的一些敏感事务进行加密外，据文件记载，官方在保护税收记录的时候，也同样广泛使用密码术。更多的证据来自许多管理手册，如 10 世纪的《大臣手册》，其中包括一些讨论密码术的章节。

管理者使用的密码表通常是前面所述的明码字母表一次简单的重排，但他们也使用包括一些其他类型字符的密码表。例如明码表中的 a 在密码表中可能被 # 所代替，b 可能被 + 号代替等等。这种替换密码有一个通用的名字叫单字母替换密码，其中密码表可以是字母也可以是符号或者两者都有。到目前为止，我们遇到的所有替换密码都属于单字母替换密码。

倘若阿拉伯人仅仅熟悉怎样使用单字母替换密码，他们就不会在密码术历史中占有如此重要的一席之地了。而事实是阿拉伯的学者不仅会使用密码，他们还能够破解密码。实际上他们发明了密码破译术，这是一门关于如何在没有密钥的情况下复原一条信息的科学。当写密码的人发明出一种新的密码编码方法时，破解密码的人就努力寻找这些方法中的弱点，从而破译出机密的信息。阿拉伯密码破译专家成功地发现了破解单字母替换密码的方

法。几个几世纪以来一直被视为无法攻破的密码终于被征服了。

也只有当一个文明的某些方面的学术达到较高的成就时，才能发明出密码破译术。这些学术包括数学、统计学和语言学。穆斯林文明为密码破译术的出现提供了一个理想的基础。由于伊斯兰人民要求在人类活动的各个方面都能做到有理可寻，而要做到这一点就离不开知识，因此每个穆斯林人都觉得有义务追求各种形式的知识，而阿巴斯王朝经济的成功使得学者在时间、金钱和物质要求方面都有了足够的保障来履行他们的义务。他们认真地从以前的文明那里获取知识，包括埃及、巴比伦、印度、中国、罗马，他们把这些文明留下的文章著作翻译成阿拉伯语供其研究。公元815年，哈里发阿尔穆蒙在巴格达建立了一座智慧之屋，作为图书馆兼翻译中心。

由于从中国学到了造纸技术，因此伊斯兰文明在获取知识的同时能够传播这些知识。纸张的生产形成了一种职业，称为“处理纸张的人”。当时每年最多能出版上万本的书籍，仅巴格达的一个郊区就有超过一百家的书店。书店里，除了一些经典著作如《一千零一夜》外，其他你能想到的任何方面的书本都有卖。这些书店是当时世界上这个最有文化气息的社会中一个不可缺少的元素。

除了自然科学，密码破译术的发明也依赖于宗教学的成长，当时在什巴拉和巴格达建有几座主要的神学学校。那里，神学家们正在校对可兰经中的穆罕默德启示录，他们对建立一个启示录的年鉴很感兴趣，于是就计算每一条启示录中各个单词的出现频率，由于某些特定单词出现的相对较晚，因而一条启示录中这些新单词的数量较多，表明这条启示录在年鉴中应处于较后的位置。神学家们同时也研究了关于穆罕默德日常语录的训诫，试图证明其中每一句话都出自其本人，他们研究单词的起源变化和句子结构，来测试某篇文章是否与穆罕默德的语言模式相一致。

重要的是，宗教学者的这些校对并没有停留在单词的水平上，

他们也分析单独的字母。他们特别发现一些字母比其他字母更普遍。字母 A 和字母 L 是阿拉伯语中最普遍的字母,部分因为该语言中有定冠词 AL,而字母 J 则仅有十分之一的出现频率。这个看似无关紧要的发现将导致密码破译术上一次伟大的突破。

尽管我们不知道是谁发现字母频率的差异可用于破译密码。但是 9 世纪的科学家阿尔－金迪对该技术做了最早的描述。他被誉为"阿拉伯人的哲学家",曾写下了 290 本书,涉及了医药、天文、数学、语言学以及音乐。他最伟大的著作直到 1987 年才在伊斯坦布尔被发现,名为《关于破译加密信息的手稿》,第一页见图 6 所示。虽然书中含有对统计学还有阿拉伯语法的详细讨论,但是阿尔－金迪的革命性的密码破译系统可压缩在两段话中。

> 如果我们知道一条加密信息所使用的语言,那么破译这条加密信息的方法就是找出用同样的语言写的一篇其他文章,大约一页纸长,然后我们计算其中每个字母的出现频率。我们将频率最高的字母标为 1 号,频率排第 2 的标为 2 号,第三标为 3 号,依次类推,直至数完样品文章中所有字母。
>
> 然后我们观察需要破译的密文,同样分类出所有的字母,找出频率最高的字母,并全部用样本文章中最高频率的字母替换。第二高频的字母用样文中 2 号代替,第三则用 3 号替换,直到密文中所有字母均已被样文中的字母替换。

用英文字母表我们很容易解释阿尔－金迪的方法。首先我们需要研究一篇或几篇一定长度的普通英文文章,建立字母表中每个字母的频度表。英语中 E 是最常见的字母,其次是 T、A 等等,如表 1 所示。然后检查待解决的密文,计算出其中每个字母的出

图 6:阿尔－金迪的《关于破译加密信息的手稿》的第一页,其中有最早被发现的“频度分析”的详细描述。

现频率。如果密文中最普遍的字母是J,那么它很可能就用来替换E的字母;如果密文中第二高频的字母是P,那么它可能是T的替换字母等等。阿尔－金迪的技术被称为"频度分析",它表明了没有必要去检验数亿条有可能的密钥,相反,通过简单的分析密文中每个字符的出现频率就有可能揭示出一条被混乱的信息。

表1:此相对频率是从报纸和小说中记录下来的。共调查100362个字母裹惯例,由H·克和F·皮波刊登在《密码系统——通信保护》上。

字母	百分比	字母	百分比
a	8.2	n	6.7
b	1.5	o	7.5
c	2.8	p	1.9
d	4.3	q	0.1
e	12.7	r	6.0
f	2.2	s	6.3
g	2.0	t	9.1
h	6.1	u	2.8
i	7.0	v	1.0
j	0.2	w	2.4
k	0.8	x	0.2
l	4.0	y	2.0
m	2.4	z	0.1

然而我们不可能无条件地应用阿尔·金迪的方法来破译密码,因为表1中的标准频率仅是个概数,不会精确地与每一篇文章的频率相符。例如有一篇短句讨论空气对非洲带斑纹的四足动物运动的影响:"From Zanzibar to Zambia and Zaire, ozone zones make zebras run zany zigzags."大意是从桑给巴尔到赞比亚和扎伊尔,这些空气新鲜的地带使得斑马以滑稽的姿态弯弯曲曲的向前跑动。对这个句子直接作频度分析就没有什么意义。通常,短文可能较明显地偏离标准频率。假如文章少于100个字母,那么用它来解密就会很困难。而另一方面,较长的文章会更可能地接近标准频

率,尽管并不总是这样。1969 年法国作家乔治斯·佩雷克写了一本 200 页的小说《逃亡》,其中没有一个含有字母 e 的单词。更令人称道的是英国小说和评论家吉尔伯特·阿代尔成功地将《逃亡》翻译成英文,而其中居然也没有一个字母 e。阿代尔将这本译著取名为《真空》,令人惊叹,值得一读。由于英文字母中最常见的字母完全没有出现,因而如果将这整本书根据单字母替换密码而进行加密的话,那么天真地试图去解密它将会受到极大阻碍。

介绍完密码破译术的第一种工具后,我将继续列举一个例子来说明怎样用频度分析破解一条密文。我已避免在本书中例举各种破解密码的例子,但对频度分析我要破例一次。这是因为频度分析并不像其听上去那么困难,也是因为它是最初的一种密码破译工具。而且,下面的例子能使我们了解密码破译者的常用方法。频度分析需要逻辑思维,但你会发现它也要求一定的策略、直觉、灵活性以及猜测。

破译一条密文

PCQ VMJYPD LBYK LYSO KBXBJXWXV BXV ZCJPO EYPD KBXBJYUXJ LBJOO KCPK. CP LBO LBCMKXPV XPV IYJKL PYDBL, QBOP KBO BXV OPVOV LBO LXRO CI SX'XJMI, KBO JCKO XPV EYKKOV LBO DJCMPV ZOICJO BYS, KXUYPD: "DJOXL EYPD, ICJ X LBCMKXPV XPV CPO PYDBLK Y BXNO ZOOP JOACMPLYPD LC UCM LBO IXZROK CI FXKL XDOK XPV LBO RODOPVK CI XPAYOPL EYPDK. SXU Y SXEO KC ZCRV XK LC AJXNO X IXNCMJ CI UCMJ SXGOKLU?"

OFYRCDMO, LXROK IJCS LBO LBCMKXPV XPV CPO PYDBLK

试想我们已经截获了这条加了密的信息。问题是要对它进行

解密。我们知道该文是用英语书写的,并已根据单字母替换密码进行了加密。但我们不知道其用的密钥。搜寻所有密钥是行不通的,因此我们决定使用频度分析。下面将一步步指导怎样破译该密文,但如果你有信心,可以略过这些,自己尝试独立地破译它。

看到这样一篇密文,无论哪个密码破译者的立即反应是先分析所有字母的频度。结果见表 2。可见,字母在出现频率上有所差异。现在的问题是,根据它们的频度,难道我们能够辨认出每个字母代表的是什么吗? 由于密文相对较短,因此我们不能机械地使用频度分析。如果就假定密文中最常见的字母 O 即代表英文中最常见的字母 e,或者密文中频率排第八的字母 Y 代表英文中排第八的字母 h,那将是天真的。不假思索地应用频度分析只会得到杂乱无章的语句。例如,第一个单词 PCQ 将被解密成 aov。

表 2:密文的频度分析

字母	频率		字母	频率	
	出现次数	百分比		出现次数	百分比
A	3	0.9	N	3	0.9
B	25	7.4	O	38	11.2
C	27	8.0	P	31	9.2
D	14	4.1	Q	2	0.6
E	5	1.5	R	6	1.8
F	2	0.6	S	7	2.1
G	1	0.3	T	0	0.0
H	0	0.0	U	6	1.8
I	11	3.3	V	18	5.3
J	18	5.3	W	1	0.3
K	26	7.7	X	34	10.1
L	25	7.4	Y	19	5.6
M	11	3.3	Z	5	1.5

然而,我们可以先将注意力放在密文中出现超过 30 次的三个字母上,即 O、X 和 P 。

我们可以比较安全地认为密文中最常见的字母可能代表英文

中最常见的字母,但不一定按照相应的次序。换句话说,我们不能肯定 O=e,X=t,以及 P=a,但我们可以做些尝试:

O=e、 t或a, X=e、 t或a, P=e、 t或a

为了有信心确定这三个最常见字母 O, X 和 P 的真实身份,我们需要对频度分析做一些细微的改进。除了简单地计算三个字母的频率外,我们还可以注意周围其他字母出现的情况。例如,字母 O 的前后有其他字母吗? 或者,字母 O 是否倾向于仅与几个特定的字母作邻居? 回答这些问题将会很好地表明字母 O 代表的是一个元音还是一个辅音。如果字母 O 代表一个元音,那它可出现在其他大多数字母的前后,而如果代表一个辅音,则会避开大多数的字母。例如,字母 e 能够与其他的几乎每一个字母组合,而字母 j 却几乎不会出现在字母 b、d、g、j、k、m、q 和 v 的两边 。

下表取密文中最常见的 O、X 和 P 三字母,列出每个字母与其他字母相邻的次数。例如 O 出现在 A 前一次,出现在 A 后零次,因此表中第一格总数为 1。字母 O 能与大多数的字母相邻,仅与 7 个字母完全不靠,因 O 行有 7 个 0。字母 X 也同样活跃,因为它除了 8 个字母以外的其他所有字母的两旁都有它的踪迹。然而字母 P 却没有那么多朋友,它一般只潜伏在几个字母的两边,与 15 个字母没有接触。这些情况表明 O 和 X 代表元音,P 代表一个辅音。

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
O	1	9	0	3	1	1	1	0	1	4	6	0	1	2	2	8	0	4	1	0	0	3	0	1	1	2
X	0	7	0	1	1	1	1	0	2	4	6	3	0	3	1	9	0	2	4	0	3	3	2	0	0	1
P	1	0	5	6	0	0	0	0	0	1	1	2	2	0	8	0	0	0	0	0	0	11	0	9	9	0

现在我们必需问自己 O 和 P 代表的分别是哪个元音。有 e 和 a 两种可能,它们是英文中最普遍的字母。但究竟是 O=e 和 X=a 呢? 还是 O=a 和 X=e 呢? 密文中有个有趣的现象是 OO 组

合出现了两次,而 XX 组合却没有。由于在一般英文文章中 ee 出现的频率比 aa 高,因此一个可能结论是 O = e,X = a 。

在此基础上,我们有信心能够辨认出密文中的两个字母。我们的结论是 X = a,事实依据是 X 在密文中以单字形式出现过,而英文中仅有两个单词有单字母组成,其中一个就是 a。密文中另一个以单字形式存在的字母是 Y,它非常可能代表英文中的另一个单字母词 i 。从一个单字母着手是标准的密码破译方式。这种特殊的技巧也只有当密文单词间还留有空格时才有效。通常,密码的作者会移去所有的空格,以便使敌方拦截者更难还原信息。

虽然单词之间有空格,但我们仍需使用下面的技巧,这种技巧对已连成一串字符的密文同样有效。一旦我们已经辨认出字母 e,使用这个技巧能使我们标出字母 h。在英语中,字母 h 经常出现在 e 的前面(如 then,they),却很少位于其后。下表显示了密文中的字符 O(我们已经认为它代表 e)出现在其他字母前后的频率。该表暗示密文中字母 B 代表 h,因为它出现在 O 前面 9 次,却没有一次位于其后。表中没有其他字母像 B 这样有着与 O 一样如此不对称的关系。

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
O后	1	0	0	1	0	1	0	0	1	0	4	0	0	0	2	5	0	0	0	0	0	2	0	1	0	0
O前	0	9	0	2	1	0	1	0	0	4	2	0	1	2	2	3	0	4	1	0	0	1	0	0	1	2

英语中每个字母都有其自己的特性,包括它的频率和与其他字母的关系。正是这种特性使我们能够确立一个字母的真实面目,哪怕它已经通过单字母替换而伪装起来。

我们现在已经明确了 4 个字母,O = e,X = a,Y = i 以及 B = h,我们可以开始将密文中的一些字母替换成明文中的字母。我仍保留将密文字母大写,明文字母小写的习惯。这有助于区分那些已被确认的字母和还待辨别的字母。

这一步虽然简单,但可以帮助我们确定其他几个字母,因为我们可从密文中猜出一些单词来。例如,英语中最常见的三字母单词是 the 和 and,因而可较容易认出密文中出现 6 次的 Lhe 和出现 5 次的 aPV。那么,L 可能代表 t,P 可能代表 n,V 可能代表 d。我们现在把密文中的这些字母换回其原来真实面目。

PCQ VMJiPD LhiK LiSe KhahJaWaV haV ZCJPe EiPD KhahJiUaJ LhJee KCPK. CP Lhe LhCMKaPV aPV liJKL PiDhL, QheP Khe haV ePVeV Lhe LaRe Cl Sa'aJMI, Khe JCKe aPV EiKKev Lhe DJCMPV ZelCJe hiS, KaUiPD: "DJeaL EiPD, ICJ a LhCMKaPV aPV CPe PiDhLK i haNe ZeeP JeACMPLiPD LC UCM Lhe laZReK Cl FaKL aDeK aPV Lhe ReDePVK Cl aPAiePL EiPDK. SaU i SaEe KC ZCRV aK LC AJaNe a laNCMJ Cl UCMJ SaGeKLU?"

eFiRCDMe, LaReK IJC5 Lhe LhCMKaPV aPV CPe PiDhLK

nCQ dMJinD thiK tiSe KhahJaWad had ZCJne EinD KhahJiUaJ thJee KCnK. Cn the thCMKand and liJKt niDht, Qhen Khe had ended the taRe Cl Sa'aJMI, Khe JCKe and EiKKed the DJCMnd ZelCJe hiS, KaUinD: "DJeat EinD, ICJ a thCMKand and Cne niDhtK i haNe Zeen JeACMntinD tC UCM the laZReK Cl FaKt aDeK and the ReDendK Cl anAient EinDK. SaU i SaEe KC ZCRd aK tC AJaNe a laNCMJ Cl UCMJ SaGeKtU?"

eFiRCDMe, taReK IJC5 the thCMKand and Cne niDhtK

一旦确定了一定数量的字母,密码破译的进展也就会很快。例如,第二句开头单词是 Cn,由于每个单词都至少含有一个元音,因此 C 一定是元音。我们只剩两个元音有待辨认,即 u 和 o,u 不符合,因而 C 一定代表 o。我们还有单词 Khe,说明 K 代表的不是 t 就是 s。但我们已知道 L = t,因此显然 K = s。确认了这两个字母后,我们再将它们带入密文中,出现了词组 thoMsand and one

niDhts。凭感觉就能猜到这是 thousand and one nights。最后一行文字似乎告诉我们这段信息来自《Tales from the Thousand and One Nights》(《一千零一夜》)。这意味着 M = u, I = f, D = g, R = l, S = m。

通过继续猜测其他的单词,我们可以确认出其他的字母。但是先来看看对于明码字母表和密码字母表我们得到了什么。这两个表形成了密钥,密码作者即用它来进行替换从而加密信息。通过确认密文中字母的真实值,我们已经有效地得到密码字母表中的一些具体细节。到目前为止,我们的收获可概括在以下的原初字母表和密码字母表中。

明码表 a b c d e f g h i j k l m n o p q r s t u v w x y z
密码表 X - - V O I D B Y - - R S P C - - J K L M - - - - -

通过检查部分的密码字母表,我们能够完成密码的破译。密码表中的序列 VOIDBY 表明密码的作者已经选了一个关键词组来作为密钥的骨架。稍微猜一下就能知道该关键词组可能是 A VOID BY GEORGES PEREC,除去其中空格和重复字母后得到 AVOIDBYGERSPC。跟随其后的密码表中的字母按照字母表的顺序继续下去,并略过关键词组中出现过的字母。但这个例子有些特殊,该密码作者没有像通常那样将关键词组放在密码字母表的最前方,而是从第三个字母开始。这可能是因为关键词组是以 A 开头,密码作者想避免将 a 加密成 A。最后,明确了密码字母表中的所有字母后,我们能够揭开整篇的密文,密码破译就此大功告成。

明码表 a b c d e f g h i j k l m n o p q r s t u v w x y z
密码表 X Z A V O I D B Y G E R S P C F H J K L M N Q T U W

在此期间，沙哈拉泽已经为沙丽亚国王生下3个儿子。到了第一千零一夜，当她讲完最后一个故事，她起身亲吻了国王面前的土，并说道："伟大的国王，我已在一千零一夜里向您讲述了古老的传说和古代君王的神话。我能斗胆向您请求一件事吧？"

选自《一千零一夜》的结尾

西方的文艺复兴

从公元800年到公元1200年，阿拉伯学者处于一种智力成就的旺盛期。与此同时，欧洲还牢牢陷在中世纪的黑暗中。当阿尔-金迪在描述密码破译术发明的时候，欧洲人仍然还在为密码编码学的基本要点奋斗着。在欧洲，鼓励对密文研究的地方也只有修道院，在那里修道士研究圣经，希望能从中找出一些隐含的意思。一直到现代还有人为此着迷。

《旧约全书》中有一些有意且明显的密码术的使用例子，中世纪的修道士对此深感兴趣。例如，《旧约全书》中有几页文章通过一种被称为阿特巴士的传统方法进行了加密。阿特巴士的原理是取一个字母，指出它位于字母表中正数第几位，再把它替换为从字母表倒数同样的位数后得到的字母。在英文中，例如a是字母表中的第一位字母，将被z即字母表中最后一位字母所代替；b则被y替换等等。事实上，阿特巴士(atbash)这个名称本身就是这种它所指的替换密码，因为其中a和t分别指希伯来字母表中的第一位字母aleph和倒数第一位字母taw，而ba和sh则代表字母表中的第二位字母beth和倒数第二位shin。关于atbash的一个例子是在耶利米书25:26和51:41，那里巴比伦塔"Babel"被换成单词

"sheshach"。"Babel"在希伯来文中由三个字母构成,第一个字母是 beth,它是希伯来文中第二位字母,被换成了倒数第二位字母 shin;第二个字母也是 beth,同样被换成了 shin;第三个字母是 lamed,是希伯来文中第十二位字母,被换为倒数第十二位字母 kaph。

阿特巴士和《圣经》中其他的密码也许仅用来增加《圣经》的神秘感,而不是隐藏什么意思,但它们足够能引起人们对真正的密码编码术的兴趣。欧洲的修道士开始重新发现古老的替换密码,同时也发明了一些密码,是他们把密码编码学重新引入到了西方文明中。

现知的第一本描述密码使用的欧洲书籍是于 13 世纪由英国圣方济会的修道士和博学家罗杰·培根所写。该书名叫《密文其实并不神奇》,它讨论了七种将信息保密的方法,并提醒道:"不用隐秘的手法写一条密文的人是愚蠢的。"

到了 14 世纪,随着炼金术士和科学家用密码来为他们的发明保密,密码术的使用开始日渐广泛。大家知道杰弗里·乔叟吗?乔叟在文学上有所成就,但他其实也是个天文学家和密码编码学家。在早期欧洲著名的几个有关密码的例子中,其中一个就是他的杰作。在他的《星球概述》一书中,他附加了题为《星球的赤道》的附录,对其中几段进行了加密。

乔叟的加密是把明文中的字母用符号来代替,例如 b 变成了 δ。第一次看见完全由奇怪的符号而不是字母构成的密文会觉得很复杂,但其本质上相当于传统的字母与字母替换,加密的过程和安全性是完全一样的。

到了 15 世纪,欧洲的密码编码术已经是一种蒸蒸日上的行业了。文艺复兴期间的艺术、科学和学术的复苏为密码编码学提供了广阔的发展空间。而政治上的尔虞我诈也愈演愈烈,这更为秘密通讯的发展提供了动力。尤其是意大利,为密码术的发展提供

了一个理想的环境。作为文艺复兴的心脏，意大利本身是由几个自治的城邦组成，每个城邦政府都希望能够胜过其他城邦。当时外交也相当频繁，每个城邦均会派大使到其他城邦政府。每个大使都从各自城邦的领导那里取到一些信息，即关于他将履行的外交政策的一些细节。相应地，每个大使也会发回他所收集到的任何信息。显然，这种双向的通讯都非常有加密的必要，因此在每个城邦都建有密码机构，每个大使都有一个密码助理。

随着密码术成为一个常规的外交工具，密码破译科学也开始在西方出现了。外交官仅熟悉建立秘密通讯所需的一些基本技能，而此时已经有人在尝试破坏这种安全性。很可能密码破译法是欧洲人独立发现的，但也不排除它是从阿拉伯国家引进的可能性。伊斯兰国家在科学和数学上的发现极大地影响了欧洲科学的再生，密码破译术或许就是流传到欧洲的一种知识。

有证据证明第一位欧洲伟大的密码破译家是乔瓦尼·索罗，他在 1506 年被任命为威尼斯人的密码助理。索罗的名气响遍整个意大利，友好城邦都会将截获的信息送到威尼斯交给索罗破译。梵蒂冈是密码破译术第二大活跃中心，它也将落到其手中的看似无懈可击的密信交给索罗破译。公元 1526 年，罗马教皇克莱门特七世送给索罗的两条加密的信息均成功地被解密，而后送返回来。当教皇自己加密的信息被佛罗伦萨人截获后，教皇送了一份复本给索罗，希望他能确定这是无法破解的。索罗声明他不能破译教皇的密码，也就暗示了佛罗伦萨人也不能破解它。不过，这或许是索罗的一个计谋，以此来迷惑梵蒂冈的密码编译家，使其对其密码的安全性产生一个错误的认识。索罗实际可能不愿指出教皇密码的弱点之处，因为那样只会促使梵蒂冈人使用更安全的密码，这样索罗也可能就无法破解了。

在欧洲其他地方，一些宫廷也开始雇用有能力的密码破译者，如费利波特·巴布，法国国王弗朗西斯一世的密码破译家。巴布因

其非凡的执着而著名，为了破解被截获的信息，他能日夜工作达数星期。但不幸的是，这使得国王有足够机会与他妻子长时间私通。到了16世纪末，随着弗朗西丝·维特的加盟，法国人进一步加强了其破解密码的能力。维特对破解西班牙的密码情有独钟。西班牙的密码编码者同欧洲其他地方的对手相比显得天真幼稚，当他们发现他们的信息对法国人而言就如水一样透明时，他们简直无法相信。西班牙国王菲利普二世不远万里来向梵蒂冈请愿，声称对维特的密码破解能力惟一的解释就是他是与魔鬼同党的一个恶魔。菲利普要求在一个红衣主教法庭上对维特魔鬼般地行为作一次审判。但教皇清楚他自己的密码破译分析家对西班牙的密码了如指掌，因而拒绝了西班牙的请愿。关于请愿的新闻很快传到各个国家的密码专家的耳中，西班牙密码编码者便成了欧洲的笑料。

西班牙的尴尬也预示着密码编码者和密码破译者之间战火的燃起。这是个过渡时期，密码编码者仍依靠单字母替换密码，而分析者开始使用频度分析来破解密码。那些仍等待发现频度分析威力的人继续相信单字母替换密码，却不知道索罗、巴布及维特等密码破译家究竟有多大的能耐来读懂他们的信息。

与此同时对单字母替换密码弱点有所警觉的国家正急于发展一个更好的密码，以有效地保护他们国家的信息不被敌方分析家恢复原样。对单字母替换密码最简单的一种改进是引进了空符号，它是指密文中的一些符号或者字母，不是用来替换实际的字母，而仅表示“空白”。例如，有人用1到99之间的数字来替换明文中的字母，那么就会有73个数字没有任何替代物，它们不代表什么，即表示“空白”。这些可作为空符号随机地插入密文中，其频率是不定的。这些空符号对联络好的密码接收人不会产生什么问题，他们知道要把这些空符号去掉，然而这却为难了敌方拦截者，因为这些符号会干扰频度分析。还有一个同样简单的改进是密码编码者在加密信息之前先有意拼错几个单词，使密码破译者很难

应用频度分析。而对方接收者知道密钥可以在复原信息后再处理那些错误的拼音。

另一种加强单字母替换密码的途径是代码的引进。代码在日常语言中有很广泛的含义,通常用来形容任何形式的秘密通讯。然而正如引言中提到的那样,它实际有个很明确的意思,仅指一种特定的替换密码。到目前,我们讨论的替换密码是指每个字母被一个不同的字母、数字或符号所代替,然而,我们可以进行更高层次的替换,以及每个单词被另一个不同的单词或符号替换,这就是代码。例如:

刺杀 = D　　将军 = E　　立即 = 08
勒索 = P　　国王 = Ω　　今天 = 73
抓住 = J　　大臣 = φ　　今晚 = 28
保护 = Z　　王子 = θ　　明天 = 43
明文 = "今晚谋杀国王"
加密后 = D - Ω - 28

看上去,代码好像比密码提供了更高的安全性,因为单词与字母相比没有那么容易屈服于频度分析。破译一个单字母替换密码你只需确定 26 个字母的真实身份,而破译一个代码,你需确定成百甚至成千个代码的意思。然而,让我们更细致地观察代码,我们就会发现它同密码相比有两大缺陷。第一,对密码而言,一旦发送者和接收者对密码表(即密钥)的 26 个字母达成共识,他们可以加密任何信息。但是对代码而言要达到同样的灵活度,他们要给明文中可能出现的成千的单词定义各自的代码,这将是件艰苦的任务。而密码表也将变成上百页的密码簿,看上去像本字典。换句话说,编辑一本密码簿将是件艰巨的工作,随身带着它也极为不便。

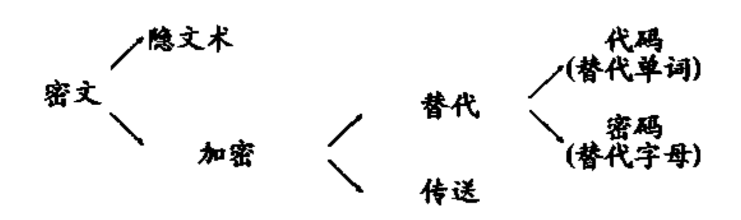


图 7:密码学及其主要分支

第二,这样一本密码簿被敌人获取之后,其后果将是灾难性的。所有加密的通讯立刻暴露在敌人面前。发送者和接收者将不得不再次经历痛苦地重新编辑一本全新的密码簿过程,而这个笨重的新册子不得不发给通讯网络上的每个人,即意味着要秘密把它送到每个城邦的每位大使手中。而相比之下,假如敌人捕获了一个密钥,就很容易编一个新的 26 个字母密码表而且也易于记忆和分发。

16 世纪,最好的密码破译师不仅能够破译密码和代码,也能够处理故意拼错的信息甚至空符号。换句话说,他们能够破解当时大多数的加密信息。他们的技能导致秘密源源不断地被揭开,这一切影响了他们主子的决定,进而在关键的时刻影响了欧洲的历史。

没有什么能比苏格兰玛丽女王更能说明密码破译学的影响。对她审判的结果完全依赖于她的密码编码者和伊丽莎白女王的密码破解者之间的斗争。玛丽毕竟是 16 世纪最著名的人物之一——苏格兰女王、法国王后、英国王位的觊觎者。然而她的命运却由一张能否被破解的纸上的信息决定着。

巴宾顿计划

1542 年 11 月 24 日，在索尔韦摩思战役中，苏格兰军队遭受英国亨利八世旗下部队的重创。苏格兰已濒临被亨利征服的边缘，詹姆斯五世的王冠也显得岌岌可危。经过这一次战役，心烦意乱的苏格兰国王在心理和生理上一溃千里，躲进了福克兰皇宫。两星期后，他的女儿玛丽的出生也未能使他从病态中恢复过来。而国王似乎一直在等待他的后继者的诞生，这样他至少能在和平中离世，从而使后人认为他尽了一个国王的责任。玛丽出生后一星期，年仅 30 岁的詹姆斯五世就去世了。还是婴儿的公主便成为苏格兰的玛丽女王。

玛丽是个早产儿，刚出生时，人们都非常担心她能否存活下去。在英国甚至传言这孩子已经死了，但这只是从英国王宫传出来的一个他们期待的想法，英国王宫一直渴望能听到任何对苏格兰稳定不利的消息。而实际上，玛丽很快就变得健康强壮，当她九个月大时，于 1543 年 9 月 9 日在斯特灵城堡的一个礼堂内举行了加冕典礼，三个伯爵代表她，分别戴着王冠，拿着权杖，配着宝剑围站在她的身旁。

玛丽女王是如此的年幼，但这使得苏格兰暂时免遭英国的侵犯。因为如果亨利八世企图袭击这样一个君主刚亡、幼主即位的国家，那他将被认为是一个缺乏风度的国王。而事实上，英国国王采取了联姻对策，即希望玛丽能嫁给他的儿子爱德华，从而使两个国家联合起来并处于都铎王室的统治之下。他开始释放索尔韦摩思战役中俘虏的苏格兰贵族，条件是他们要为苏格兰与英国的联合去活动。

但是，苏格兰王宫在考虑之后拒绝了亨利的提议，而赞成玛丽

与法国太子弗朗西斯的婚姻。苏格兰选择与同是罗马天主教的国家联合,玛丽的母亲玛丽奥夫吉斯对这个决定感到满意,因为她自己与詹姆斯五世的婚姻就巩固了苏格兰和法国的关系。玛丽和弗朗西斯都是小孩,但他们最终要结婚,弗朗西斯将继承法国的王位,而玛丽则成为他的王后,苏格兰和法国从而联合在一起。其间,法国将保护苏格兰,抵制英国的任何进攻。

这种保护的诺言得到了验证,特别是亨利八世放弃了外交而采用胁迫手段,试图说服苏格兰,他的儿子更值得玛丽女王嫁给他。他的军队沿着边界不断制造侵略行为——毁坏庄稼、烧毁村庄、袭击城镇。这种“粗暴的联姻”到了1547年亨利去世后还在继续。在他儿子爱德华六世的支持下,这些小规模的进攻终于引发了平客克流夫战役,苏格兰军队被挫败。这场战斗之后,苏格兰王室决定让玛丽离开苏格兰前往法国,以避开英国的威胁,同时在那里她还可以准备与弗朗西斯的婚姻。1548年8月7日,玛丽启航前往罗索夫港口,当时她才6岁。

玛丽在法国王宫的最初几年是她一生中最悠闲的时光。身处豪宅之中,她开始爱上她未来的丈夫:法国皇太子。16岁那年,他们结婚了,第二年弗朗西斯和玛丽分别成了法国的国王和王后。一切似乎都是在为她风光地返回苏格兰作准备,然而,她那健康状况一直不佳的丈夫却得了重病。从小就有的一种耳部感染开始恶化,炎症向脑部扩散,并出现了脓肿。1560年,登基不到一年,弗朗西斯就去世了,玛丽也就成了寡妇。

从那时开始,玛丽的生活开始接二连三地受到打击。她于1561年回到苏格兰,却发现苏格兰已经改变了。在她离位期间,她坚定了对天主教的信仰,而她的臣民却越来越多地走向新教教堂。玛丽默默忍受着这一切,起初统治得还较为成功。但在1565年,她嫁给了她的表亲亨利·司徒瓦特,即达恩利伯爵,这一行为使她陷入一连串的恶运之中。达恩利伯爵生性邪恶、残忍,他对权力

的贪婪使玛丽失去了苏格兰贵族对她的忠诚。第二年，玛丽亲身体验了她丈夫野蛮的天性带来的恐怖，达恩利当着她的面杀了她的秘书大卫·利齐欧。事情已很明显，为了苏格兰的利益，必需得除掉达恩利。关于是玛丽还是苏格兰贵族策划了这起谋杀，历史学家有所争论。但不管怎样，在 1567 年 2 月 9 日的晚上，达恩利的房屋突然爆炸，当他试图逃出时却因窒息而死于非命。这场婚姻的惟一的结果是留下了一个儿子即继位者：詹姆斯。

玛丽再婚的对象是詹姆斯·赫伯恩，即第四任波斯维尔伯爵。这次婚姻也很失败。1567 年的秋天，苏格兰新教贵族们再也不对信奉天主教的女王抱有什么幻想，他们流放了波斯维尔并监禁了玛丽，强迫她让位给她十四个月大的儿子詹姆斯六世，而她同父异母的兄弟莫里伯爵则为摄政王。第二年，玛丽从狱中逃出，聚集了一支由保皇党组成的六千人的军队，准备为夺回她的王冠作最后一搏。她的军队在靠近格拉斯哥的一个名叫朗赛德小村庄里遭遇了摄政王的军队，玛丽就在附近的一个山顶上目睹了这场战斗。虽然她的军队在数量上占优势，但他们缺乏纪律。玛丽亲眼看到她的军队被扯裂成两半，等到她发现失败是在所难免的时候，她逃跑了。理想的路线应该是先向东到达海岸，再前往法国，但这意味着她拱手把权力让给了她同父异母的兄弟。因此，玛丽反向南去了英国，她希望她的表亲伊丽莎白一世能够为她提供庇护。

其实，玛丽下了一个可怕的决定。伊丽莎白带给玛丽的仅是个囚犯的下场。表面上声称逮捕玛丽是因为她与达恩利的谋杀有关，但真正的原因其实是玛丽对伊丽莎白构成了一个威胁，因为英国天主教徒认为玛丽才是英国真正的王后。玛丽曾经通过她的祖母，亨利八世的姐姐玛格丽特·都铎之口对王位有过提及，但亨利最后一个存活的子女，伊丽莎白一世，似乎先于玛丽有此要求。然而，根据天主教徒的说法，伊丽莎白是个私生子，因为她是亨利的第二任妻子博林·安妮的女儿，亨利不顾教皇的反对与阿拉贡·凯

瑟琳离婚后娶了博林·安妮。英国天主教并不承认亨利八世的离婚,也不认可他与博林·安妮自许的婚姻,当然也不能接受他们的女儿伊丽莎白成为王后。天主教把伊丽莎白视为一个篡位的私生女。

玛丽先后被囚禁在许多个城堡和庄园中。虽然伊丽莎白把她看作是英国最危险的人物之一,但许多英国人也承认他们仰慕玛丽典雅的举止,她过人的智慧以及她惊人的美丽。伊丽莎白的首席顾问威廉·西赛尔曾提到"她带给所有男人那迷人甜蜜的快乐"。西赛尔的使者尼古拉斯·怀特也作过相似的评论:"她有着诱人的举止,一口优美的苏格兰语音,温柔婉转的外表下隐藏着过人的智慧。"但是,随着时光流逝,玛丽的容貌也越显黯淡,健康也每况愈下,她开始失去希望。她的狱卒埃米亚斯·波利特爵士是个清教徒,并不为她的魅力所动,而且愈加苛刻地对待她。

到了 1586 年,经过了 18 年的监禁,玛丽失去了她所有的特权。她被软禁在斯塔弗德施的察特里庄园,不再允许喝巴克斯顿的水,而那里的水能帮助她减轻疾病不断骚扰所带来的痛苦。在玛丽最后一次去巴克斯顿的时候,她用钻石在一块窗玻璃上刻下了这么一句话:"巴克斯顿,你的温水使你闻名遐迩,但恐怕我再也不能来看你了——别了。"似乎玛丽已猜到她将失去她仍有的那一点自由。而玛丽那 19 岁的儿子苏格兰詹姆斯六世的行为更加重了玛丽心灵上的痛苦。她一直盼望能有一天逃离这里,返回苏格兰与她那从一岁起就曾未谋面的儿子共享权利。然而,詹姆斯却对母亲没有任何亲情之心。他自幼被玛丽的敌人抚养大,并得知母亲曾经为了她的情人而谋杀了他的父亲。因而詹姆斯鄙视他的母亲,担心她回来之后会夺去他的王冠。他甚至毫不疑虑地向关押他母亲,并年长他 30 岁的伊丽莎白一世求婚,虽然伊丽莎白婉言拒绝了他的请求,但可见他对他母亲的憎恨之深。

玛丽写信给她的儿子试图赢回他的心,但她的信从未能到达

苏格兰地界。此时玛丽比以前更加被隔离起来,她所有发出的信件都被没收了,所有寄来的信件也都被狱卒扣押起来。玛丽的精神低落到极点。正是在这种绝望的时候(即 1586 年 6 月 6 日),玛丽惊奇地收到了一包裹的信件。

这些信来自欧洲大陆上玛丽的支持者们,他们通过吉尔伯特·吉法德之手带进了她的监狱。吉尔伯特·吉法德是个天主教徒,于 1577 年离开英格兰,在罗马的英国学院被培养成一个牧师。1585 年,他一回到英国,就非常渴望能为玛丽效劳,他立刻去接触在伦敦的法国使者,那儿积压着一堆给玛丽的信件。使者知道如果他们按照普通的方法送去这些信,玛丽将永远不会看到。而吉法德声称他能把这些信弄进察特里庄园,并保证他言出必行。于是第一批信件就到了玛丽手中,吉法德也就成了一个信使,不仅把信息传给玛丽,还负责玛丽的回信。他用了一个非常巧妙的方法将这些信偷偷送进了察特里庄园。他先把信件交给当地的一个啤酒制造商,啤酒制造商将信用皮纸包起来,然后藏进一个中空的啤酒桶的塞子里面,再将带有这个塞子的一桶啤酒送进察特里庄园,在那儿,玛丽的一个仆人会打开这个塞子,并把其中的东西交给苏格兰女王。这种方法同样也隐秘地把玛丽的信带出察特里庄园。

此时,在伦敦的一个酒馆里,一个营救玛丽的计划正在酝酿着,可玛丽自己还不知道。这项计划的中心人物是安东尼·巴宾顿,他年仅 24 岁,却因英俊、富有魅力以及诙谐的个性而小有名气。然而,他的仰慕者没有意识到,巴宾顿深深地痛恨着这个国家的社会制度,因为它迫害他与他的家庭以及他信仰的国教。国家反天主教的政策使恐怖气氛不断升级,天主教教父被指控犯有叛国罪,任何隐藏他们的人一经发现就会被处死,假如没死就开膛。天主教被正式取缔,那些对教皇还抱有忠心的家庭被迫要缴纳难以承受的重税。巴宾顿的曾祖父达西伯爵就曾因涉嫌参与反抗亨利八世的朝圣叛乱而被砍头,这更加剧了巴宾顿的仇恨。

1586年3月的一个夜晚,巴宾顿和他的同道者聚集在一个酒馆里开始谋划。历史学家菲利普·卡拉曼后来评论道:“巴宾顿以他特别的魅力和个性拉拢了许多与其地位相当的年轻绅士,为了捍卫危机中的天主教,他显得特别豪放大胆,敢做敢为,只要能推进天主教事业,他随时都可以赴汤蹈火。”在接下来几个月中,这项雄心勃勃的计划渐渐成熟,其中包括释放苏格兰玛丽女王,刺杀伊丽莎白女王,并在国外支持下在国内发动叛乱。同谋者们都一致认为只有得到玛丽的许可,巴宾顿计划才能进行,但却没有可行的办法与玛丽联系。1586年6月6日,吉法德来到巴宾顿的住处,他带来玛丽的一封信,信中解释她已从巴黎的支持者那里听说了关于巴宾顿的事情,希望能听到他的回音。巴宾顿写了一封详细的回信,信中描述了他的计划,并提到教皇庇护五世已于1570年将伊丽莎白逐出了教会,刺杀她将是合法的。

> 我和10位绅士还有100名跟随者将把您从您的敌人的手中解救出来。我们认为伊丽莎白是一个篡位的女王,她已被逐出教会,我们有6位贵族,都是我的密友,他们都忠心于天主教并为陛下服务。

同往常一样,为了骗过玛丽的看守,吉法德将信件藏进了啤酒桶的塞子中。这可以看作是一种隐文术,因为信件是隐藏的。巴宾顿这次特别地防范,还将信件进行了加密,这样即使信被玛丽的狱卒截获,也不能读懂其中内容而暴露其中的计划。他使用的密码不是简单的单字母替换密码,而是一种代码与密码的组合,图8所示。它包括23个用来替换字母表中字母的符号(不包括j、v和w)和35个代表单词或词组的符号,另外,还有四个空符号(ℋ.⌐.⅃.ɗ.)和一个σ̄符,它们表示其后所接的符号代表一个双字母。

吉法德年纪虽然还小，甚至比巴宾顿还年轻，但他对于送信却很自信。科尔汀、皮尔特和科马里斯都是他的别名，以避免他人的怀疑。他和天主教之间的密切关系使他在伦敦和察特里庄园均有许多安全的住处。然而，吉法德每次来往察特里庄园，他都要绕道去往另一个地方。其实，吉法德表面上是充当玛丽的密探，他实际上是一个双重间谍。在 1585 年返回英格兰之前，他就写信给伊丽莎白女王的首席秘书弗朗西斯·沃尔辛厄姆爵士，希望能为他效劳。吉法德认识到他的天主教背景可以很好地掩护他渗透到反对女王的阴谋中。在他给沃尔辛厄姆的信中写道："我听说了关于您所做的工作，我想为您效劳，我在危险面前不会有任何顾虑和害怕。无论您要我做什么，我都会圆满完成。"

a b c d e f g h i k l m n o p q r s t u x y z

Nulles　　Dowbleth

and for with that if but where as of the from by

so not when there this in wich is what say me my wyrt

send lie receave bearer I pray you Mte your name myne

图 8：苏格兰玛丽女王的信，包含密码字母表和密码。

沃尔辛厄姆是伊丽莎白手下最冷酷的一位大臣，同时也是负责君主安全的间谍首脑。他接管了一个小的间谍网络后迅速把它扩展到整个欧洲大陆，因为欧洲大陆正酝酿着许多反对伊丽莎白的阴谋。在他死后，发现他一直以来收到定期来自法国、德国、意

大利、西班牙以及低地国家的报告，他还同伊斯坦布尔、阿尔及尔和的黎波里三座城市保持信息联系。

沃尔辛厄姆把吉法德收为间谍，实际上正是沃尔辛厄姆命令吉法德去接近法国使者，主动作为他的信使。每次吉法德拿到一条送往玛丽的或玛丽送回的信息，他先把它拿给沃尔辛厄姆。这个警觉的间谍头目将信传给专门负责伪造的手下，他们拆开每一封信，做一个复件，再用同样的邮票封好原信后交回吉法德。这封看似没有触动的信件将送到玛丽或其通信者的手中，他们对这封信经历的事却一概不知。

当吉法德将巴宾顿给玛丽的信交给沃尔辛厄姆时，首要的任务是要对它解密。沃尔辛厄姆曾读过由意大利数学家及密码编码学家吉罗拉摩·卡达诺(吉罗拉摩·卡达诺在书中附带提及了一种基于触感的盲人识字法，他其实是后来布莱叶盲文法的先驱)写的一本书，所以对密码和代码已有一些了解。卡达诺的书虽然引起了沃尔辛厄姆的兴趣，但却没有引起他的重视。直到比利时佛兰德的密码破译家菲利普·范·马尼克斯使他真正觉得有一位专门负责破译密码的人在其左右是多么的必要。1577 年西班牙的菲利普王使用密信与他同是天主教的同父异母兄弟的唐·约翰联系，唐·约翰正控制着荷兰的大半部分。菲利普信中描述了入侵英格兰的计划，可是信被威廉姆截住，随后交给了他的密码助理马尼克斯。马尼克斯破译出了其中的计划，威廉姆就把消息传给了在欧洲间谍网工作的英国间谍丹尼尔罗格斯，该间谍遂警告沃尔辛厄姆敌军侵犯的企图。英国于是加强了它的防卫，粉碎了敌人进攻的计划。

现在，沃尔辛厄姆充分认识到了密码破译术的价值，他在伦敦建了一座密码学校，并雇佣汤姆斯·菲利普斯作为他的密码助理。菲利普斯是个精瘦的矮个子，看上去有三十岁，近视、黄头发衬着黄胡须，脸上还留有天花的痕迹。他是一个语言学家，能说法语、

意大利语、西班牙语、拉丁语和德语，更为重要的是他还是欧洲最好的密码破译家。

一拿到来往于玛丽的消息，菲利普斯就迫不及待地研究它。他是个密码破译大师，对他来说，找到答案只是一个时间的问题。他为所有字符建了一张频度表，并为最常出现的字符提出了可能替换它们的值。当某种途径行不通时，他可以尝试其他可能的替换。逐渐地，他能够识别专门迷惑人的空字符，并把它们排除到一边。最终剩下的就是一些代码，可根据上下文猜出它们的含义。

当菲利普斯破译了巴宾顿给玛丽的信后，显然明白这是刺杀伊丽莎白的一个计划。他马上把这个罪证传给了他的主人。沃尔辛厄姆此时完全可以给巴宾顿来个措手不及，但他却按兵不动，希望玛丽能够回信并签署这个计划，到时玛丽也将罪责难逃。沃尔辛厄姆早就盼望苏格兰玛丽女王的死期，但他知道伊丽莎白不太愿意处死她的表亲。然而，如果他能够证明是玛丽批准刺杀伊丽莎白的计划，那么他的女王陛下必将同意处死他的天主教对头。沃尔辛厄姆的目的也就达到了。

7 月 17 日，玛丽回信给了巴宾顿，这等于给自己签了死刑判决书。她特别提到关于计划的“设计”问题，表示她应该在刺杀伊丽莎白之前或者刺杀的同时被解救出来，否则消息一旦传到她的狱卒那里，伊丽莎白可能先杀了她。这封信在到达巴宾顿之前，照例先去了菲利普斯那里。有了以前的经验，他毫不费劲地破译了这封信，并标上了一个符号“Π”——绞刑架的标志。

沃尔辛厄姆有了他所需的足够证据来逮捕玛丽和巴宾顿，但他还是不满意。为了彻底地破坏这个阴谋，他需要所有参与人的名字。他要菲利普在玛丽的信后伪造一个附言，诱使巴宾顿报出所有名字。菲利普还有一项才能：他还是个模仿师，据说他只要看一眼别人的手迹，就仿造出与其一样的笔迹来。图 9 就是他加在玛丽信后的附言。她可以用图 8 玛丽定义的代码和密码表来解

密,其明文如下:

> 我很愿意知道这六个绅士的名字和资历。这样我或许能够根据这些进一步给你一些建议,并且可以不时地告诉你该如何行动。

苏格兰玛丽女王的密码清楚地说明了使用一个脆弱的密码有时比完全不用密码还糟糕。玛丽和巴宾顿之间毫无顾虑地直接交流计划,因为他们相信他们的通讯是安全的。而如果他们公开地通信,他们将以一种更谨慎的方法来提及他们的计划。而且,他们对其密码的信任使得他们特别轻易地接受了菲利普的伪作。发送者和接收者对他们密码的隐秘性是如此地相信,以至他们认为敌人是绝不可能模仿他们的密码来加入这一段伪造的密文进去。正确使用一个牢固的密码当然会有利于发送者和接收者,但错误使用一个脆弱的密码却会使人对安全性产生一种错觉。

巴宾顿收到玛丽的信和附言不久,需要去国外组织军队入侵,也就必须到沃尔辛厄姆的有关部门那里登记以取得护照。这将是一个很好的时机去逮捕这个叛国者,但是护照登记办公室里的约翰·斯丘达莫尔没料到全英格兰头号通缉的叛国者会出现在他的门前。由于没有人手,斯丘达莫尔将还蒙在鼓里的巴宾顿带到附近的一个酒馆,等待他的助手去叫一队士兵。不久一个便条送到酒馆,告诉斯丘达莫尔是逮捕巴宾顿的时候了,然而巴宾顿看到了便条,他假装随意地说他去付啤酒和菜钱,站起来把剑和外套放在桌子上,表明他很快就回来,而自己从后门溜出去逃跑了。先跑到圣约翰森林,再去往哈罗。他努力地化装自己,把头发削短,脸上涂上胡桃汁以掩饰其贵族背景。但他只躲过了 15 天,8 月 15 日他和他的 6 个同伙被抓到,带回了伦敦。全市的教堂响起胜利的钟声。对他们的刑罚真是恐怖到了极点,用伊丽莎白时期史学家

威廉姆·卡登的话就是："他们都被砍头，凡同他们有关系的有的被砍头，有的被活体开膛，还有的被卸成四块。"

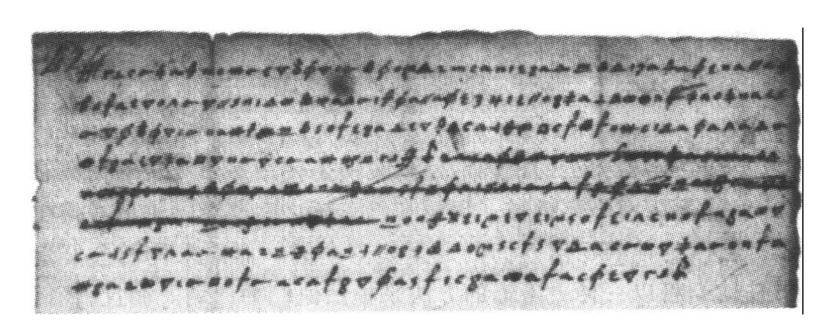


图 9：托马斯·菲利普加在玛丽信后的附言，它可以用图 8 中玛丽定义的代码和密码表来解密

与此同时即(8 月 11 日)，苏格兰玛丽女王和她的随从被特许可在察特里庄园的土地上骑马。当玛丽穿过荒野时，看见有几匹马驰来，她立刻想到这一定是巴宾顿派人来救她的。但很快又发现他们是来逮捕她而不是释放她的。玛丽因涉嫌巴宾顿计划，被指控有"刺杀行为"，1584 年国会特别制定并通过这个罪名用来起诉任何涉嫌阴谋对抗伊丽莎白的人。

对玛丽的审判在福斯灵海城堡进行，这是个阴暗昏涩的地方，位于英格兰东部城防的中部。审判于 10 月 15 日开始，有两个主法官，四个从法官，国务大臣、财政大臣、沃尔辛厄姆以及其他伯爵，爵士和男爵也来到现场。法庭后面还空出些地方给旁观者们，包括当地居民和各官员的仆人，他们都希望看见被羞辱的苏格兰女王作出请求原谅，饶她一命的样子。然而，玛丽女王自始至终都保持着庄重和镇静。她主要的辩护就是拒绝与巴宾顿有任何关系的指控，"难道要我对那几个狂人的罪恶计划负责吗?"玛丽声称，"我既不知道内情，也没参与。"但她的称述却丝毫不能影响那些对

她不利的证据。

玛丽和巴宾顿依靠一个密码来保密他们的计划，但在他们生活的时代，密码破译术正逐渐消弱密码编码术的成就。尽管他们的密码对于一个外行来说足以起到保护的作用，但遇到一个密码破译专家却一点机会也没有。在观众席上坐着菲利普，静静地看着法庭上出示的证据，正是他魔术般地从密信中挖出了这些证据。

审判进行到第二天，玛丽继续否认与巴宾顿的关系。当审判结束时，她让法官来决定她的命运并预先宽恕了他们，因为结果其实是显然的。十天以后，全法院成员聚集在威斯敏斯特教堂，定下结论：玛丽从6月1日起就一直幻想并预谋刺杀英格兰女王。他们建议应判死刑，伊丽莎白签署了死刑判决。

1587年2月8日，在福斯灵海城堡的大厅里，三百人聚集在此观看了玛丽的处决。沃尔辛厄姆决定要尽可能地降低玛丽作为一个殉教者而死的影响，因此他决定命令焚烧掉断头台上的枕木、玛丽的衣服以及一切与砍首有关的东西，以免人们把它们作为神圣的遗物。他也在处决玛丽后的一个星期里为他的女婿西尔·菲丽普·西德尼安排了一次隆重的葬礼。西德尼死于在荷兰与天主教的一次战斗中，是个公众英雄。沃尔辛厄姆认为用一个壮观的队列游行来纪念他，将会减弱某些人对玛丽的同情。然而，玛丽也同时决定在她最后时刻视死如归，以此来激励其后继者。

当彼得伯勒牧师开始祷告时，玛丽大声地朗读自己的祈祷文，为英国天主教堂祷告，为她的儿子，为伊丽莎白祷告。心里念着家族格言"我的结束就是我的开始"，玛丽镇定自若，走上了断头台。刽子手请求她的宽恕，她答道："我从心里原谅你，因为现在我希望你能把我所有的烦恼做一个了结。"

理查德·文菲尔德在他的《苏格兰女王的最后一天》中描述了她最后的时刻：

然后她非常安静地躺在行刑台上，伸展开她的手臂和双腿。大声朗读三四次主祷文，到了最后的时刻，一个行刑者用一支手轻轻地拥着她，另一个砍下她头之前用斧子挥舞了两下，她在被砍下头时发出了极小的声音，没有任何动作。她的头被砍下之后，嘴唇上下颤动了半个小时。然后一个行刑者用力地想摘下她衣服里的勋位章，却卡在她的头和肩之间，最后也没能从她的尸体上摘下来。

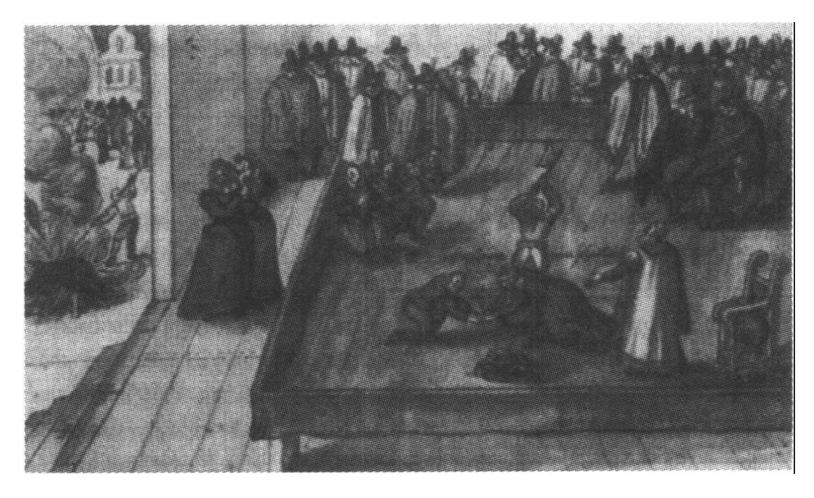


图 10:苏格兰玛丽女王的行刑。

第二章 不可破译的密码

几个世纪以来,仅是单字母替换密码已足以保证信息的安全。然而,从阿拉伯开始继而进入欧洲的频度分析,这些先进的解密技术破坏了单字母替换密码的安全。苏格兰玛丽女王的悲惨死刑则对这种单字母替换密码的弱点做了戏剧化的诠释。显然在这场密码编码者和密码破译者之间的战争中,是密码破译者占了上风。任何发送加密消息的人都不得不承认,敌方一个熟练解码员就有可能截取并译解他们最宝贵的机密。

责任明显地落在了密码编码者的肩上,他们必须编出一种更强大的新密码,这种密码能在智慧上战胜密码破译师。虽然这样的密码直到16世纪末才出现,但是它的起源却可追溯到15世纪佛罗伦萨的博学者里昂巴蒂斯特·阿尔伯提。阿尔伯提生于1404年,是文艺复兴的领导人物之一。他是一个画家、作曲家、诗人和哲学家。他在历史上首次系统地分析了透视画法,他著文论述了家蝇,并且为他的狗做过悼文。不过他最广为人知的身份要算是建筑师,他曾经设计了罗马第一座喷泉。第一本印刷出版的关于建筑学的书也是他写的,这本书大大促进了歌特式建筑类型向文艺复兴时期设计类型的转变。

15世纪60年代的某一天,当阿尔伯提漫步在梵蒂冈的花园

里时,意外地见到了他的朋友,罗马教皇的秘书莱奥纳多·戴托。后者开始和他聊起了关于密码编码学的一些精要。这次偶然的对话促使阿尔伯提就这方面写了一篇文章,概述了他所认为的新式密码。在那时,所有的替换密码都需要专一的密码表来把每条信息译成密码。然而,阿尔伯提建议用两个或两个以上的密码表,在将信息译成密码时交替使用,以迷惑一些密码破译师。

明码表 a b c d e f g h i j k l m n o p q r s t u v w x y z
密码表1 F Z B V K I X A Y M E P L S D H J O R G N Q C U T W
密码表2 G O X B F W T H Q I L A P Z J D E S V Y C R K U H N

例如,我们这里有两个可能的密码表,可通过轮流使用它们来加密一条信息。要加密"hello",我们可根据第一个密码表加密第一个字母,如此一来 h 变成了 A,再根据第二个密码表加密第二个字母,这样 e 变成了 F。在加密第三个字母时又回到第一个密码表,加密第四个字母时再用第二个密码表,这就意味着第一个 l 变成 P,第二个 l 变成 A。最后一个字母 o 根据第一个密码表被加密成 D,完整的密文则是 AFPAD。阿尔伯提系统最关键的优点在于明文里的同一字母不一定以相同的字母出现在密文里。因此"hello"里重复的"l"在不同的情形下被加密成不同的字母。同样,在密码里重复的"A"在不同的情形下代表不同的明文字母,第一个代表"h",第二个代表"l"。

虽然阿尔伯提是一千年来在加密问题上取得了最重大突破的人,但是他未能把他的理念发展成一个完全成形的加密系统。这个任务由一群不同的人在他想法的基础之上完成。首先是约翰尼斯·特里色米斯,一个于 1462 年出生的德国修道士;接着是乔瓦尼·波特,1535 年出生,是个意大利科学家;最后是布莱兹·德·维热纳尔,生于 1523 年,是名法国外交官。维热纳尔在他 26 岁的时



图 11:布莱兹·德·维热纳尔

候被派遣到罗马担任为期两年的外交官，这时他开始熟悉阿尔伯提、特里色米斯和波特的著作。开始时，他对密码编码学的兴趣完全出于实用的目的，他把这些与他的外交工作联系在一起。直到他 39 岁时，维热纳尔认为他已积累了足够的钱财可以使他放弃当时的工作而全身投入到研究中。直到这时，他才详细地研究阿尔伯提、特里色米斯和波特的思想，并最终编出了一个系统的、更为有效的新密码。

表 3：维热纳尔方阵

Plain	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

虽然阿尔伯提、特里色米斯和波特都做出了各自重要的贡献，但密码最终的形式是由维热纳尔所确立，因而还是以维热纳尔密码而著称。维热纳尔密码的长处在于它用的是 26 个不同的密码表而不是单单一个密码表来加密信息。加密的第一步是画一个所谓的维热纳尔方阵，如表 3 所示，明码表下面是 26 个密码表，每个表相对于前一个发生一次移位。因此，第一行实际上进行了一次恺撒一位移位，同样第二行是由恺撒二位移位产出的一个密码表，依此类推。方阵的最顶行小写字母代表的是明文字母。你可以根据 26 个密码表中任意一个来加密每个明文字母。例如如果选择第二个密码表，那么字母 a 就被加密为 C，但如果使用第 12 个密码表，a 被加密成 M。

假如发送者仅使用密码表中的某一个来加密一个完整的信息，这实际上就是一个简单的恺撒密码，作为一个非常弱的加密形式，很容易被敌方拦截者破解。然而，在维热纳尔密码中，却是使用维热纳尔方阵中不同的行(即不同的密码表)来加密信息中不同的字母。也就是说，发送者可能是根据第 5 行来加密明文中第一个字母，而根据第 14 行来加密第二个字母，根据第 21 行来加密第三个字母等等。

要复原一个信息，接受者需要知道每个字母是根据维热纳尔方阵中哪一行来加密，因此必需有一个统一的可行切换程序。而使用一个关键词就可以做到这一点。为了说明一个关键词是如何与维热纳尔方阵一起使用来加密一段信息，我们来实践一下。我们用关键词 WHITE 来加密 divert troops to east ridge(“转移部队到东山”)这句话。首先，对应明文，一遍一遍地拼写关键词，直到明文中每个字母都对应于关键词中的某个字母。然后，按如下方式产生密文，加密第一个字母 d：找出其对应的关键词中的字母是 W，在维热纳尔方阵中找出以 W 开始的行是 22 行，找到以 d 开始列和以 W 开始行的交界处，发现是字母 Z，因而明文中的字母 d

就被替换为密文中的 Z。

关键词	W H I T E W H I T E W H I T E W H I T E W H I
明　文	d i v e r t t r o o p s t o e a s t r i d g e
密　文	Z P D X V P A Z H S L Z B H I W Z B K M Z N M

Plain	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

表 4:一个维热纳尔方阵,其中黑体字是由关键词 WHITE 表示的。加密应在五个黑体密码字母表之间转换。

重复以上的过程就可加密信息中第二个字母 i,其对应的关键字母是 H,因而它将根据维热纳尔方阵中另一不同行来加密:H 行(行 7)是一个新的密码表。要加密i, 我们找到以 i 开始的那一列

与以 H 开始的那一行的交界,发现是字母 P。因而明文中的字母 i 在密文中用 P 来表示。关键词中的每个字母表示维热纳尔方阵中一个特定的密码表。因为关键词有 5 个字母,因此发送者循环使用维热纳尔方阵中的 5 行来加密信息。信息中的第 5 个字母根据关键词的第 5 个字母加密,但是加密信息中第 6 个字母时,我们必须回到关键词的第 1 个字母。一个较长的关键词,或者一个关键词组将使用更多的行,增加了密码复杂性。图 4 表示的是一个维热纳尔方阵,其中显黑的是由关键词 WHITE 决定的 5 行(或者说,5 个密码表)。

维热纳尔方阵最大的优点在于它克制了第一章描述的频度分析。例如,一个密码破译师对这样的一篇密文使用频度分析时通常是先确定密文中最常见的字母,在这里是 Z,然后假定它代表的是英语中最常见的字母 e。很显然密码破译师犯了一个错误。事实上,这个密文中出现 7 次的字母每次都代表的是明文中不同的字母,这就极大地迷惑了密码破译师。同样会令密码破译师困惑的是明文中出现 7 次的字母在密文中被不同的字母替换。例如,在 troops 中重复出现的字母 o 被两个不同的字母所代替,oo 加密成 HS。

除了不惧怕频度分析,维热纳尔密码还具有数目众多的密钥。发送者和接收者可以使用字典中任一个单词,或单词组合,或者虚构的词作为关键词。一个密码破译师是不能通过搜索所有可能的密钥来破解信息,因为密钥数量简直是太多了。

1586 年,维热纳尔出版了一本关于密文的书《密码理论》,他的事业也达到了巅峰。可笑的是,这一年托玛斯·菲利比斯正在破解苏格兰玛丽女王的密码。如果玛丽的助理读了这本书,他就会

知道维热纳尔密码,玛丽给巴宾顿的信息就将挫败菲利普斯,她或许会捡回一条命。

维热纳尔密码的确提供了很好的安全保障,它似乎很快会被全欧洲的密码助理所接受。然而,密码助理们似乎都摒弃了维热纳尔密码。在接下来的两个世纪里,这个看上去没有任何漏洞的加密系统很大程度上都被忽略了。

从维热纳尔密码的冷落到铁面人

在维热纳尔密码出现以前的传统替换密码被称为单字母替换密码,因为它们对每个信息仅使用一个密码表。相反,维热纳尔密码属于一类叫多字母替换密码的一种,因为对每个信息它使用多个密码表。正是维热纳尔密码的多字母特性带给它高度的安全性,但是这也导致使用时更加复杂。维热纳尔密码需要耗费更多的精力,这一点阻止了许多人使用它。

17 世纪,诸多的原因仍使得单字母替换密码成为主流。如果你想确保你的仆人不会读你的私人信件,或者如果你不想让你的妻子或丈夫偷看你的日记,那么这个古老的加密形式将是完美的。单字母替换密码使用起来快速、简单,对付一些非专业的人是绰绰有余。

事实上,简单的单字母替换密码以各种形式存在了将近几个世纪。对于一些较正式的应用来说,例如军事和政府通讯,他们的安全性是放在第一位的,直接使用单字母替换密码显然是不够的。专业密码编码师在和专业密码破译师的斗争中需要一些更好的东西,然而他们仍然不愿使用多字母替换密码,因为它太复杂。军事通讯特别需要速度和简便,一个外交办公室每天可能发送或接收上百条的信息,因此时间是关键所在。于是密码编码师就寻找一

种折中的密码,它应该比单字母替换密码更难破解,但比多字母替换密码更容易使用。

在众多的选择中,有一种相当有效的密码叫同音替换密码。其中,每个字母有不同数量的替代者,替代者的数量与每个字母的频率成正比。例如,字母 a 在书面英语中大约占到 8%的比例,因此我们可以分配 8 个符号来代表它。明文中出现的每个字母 a 在密文可以被 8 个符号中的任一个替换,因此在加密完之后,每个符号将占到密文的 1%。同样,字母 b 在英语中大概占 2%,因此我们分配 2 个符号代表它。每次字母 b 在明文中出现的时候,它可以被两个符号中的一个代替,加密后,每个符号将占到密文的 1%的数量。就这样我们根据字母表给每个字母分配不同数量的符号直到字母 z。字母 z 由于很少见,因此只有一个符号替代物。在表 5 给出的例子中,密码表中的替代符号用 2 位整数表示,从中可见明码表中的不同字母根据各自的使用频率有 1 到 12 个替换物。

我们可以想像对应明文字母 a 的所有整数在密文中实际上都代表同一个发音,就是字母 a 的发音。因此同音替换密码(homophonic substitution)这个词有一定的意义,homos 的意思是“相同的”,phonos 意思是“发音”。为一些常见的字母提供了几个替换选择这就平衡了密文中字符的频度。如果我们使用表 5 来加密一段信息,那么每个数字在整篇文章中都大约占 1%的比例。如果所有的符号在频度上都是一样的,那么通过频度分析进行的任何攻击将是徒劳的。那么,这是不是已具有绝对的安全性?不是!

聪明的密码破译师仍能在这样的密文中找到一些细微的线索。正如在第一章我们看到的,英语中的每个字母都有自己的特性,这种特性就是该字母与其他字母之间的关系。即使是在同音替换密码中,这些特性也可以被利用。英语中关于这种特性最极端的例子是字母 q,它的后面只能接一个字母就是 u。如果我们正在尝试破解一篇密文,我们知道字母 q 在英文中相对少见,因此很

可能只有一个符号来代替它。我们也知道字母 u 在英语中大概占 3%的比例，因而可能有三个符号可以用来替换它。因此如果我们发现密文中一个符号后面总是跟着三个特定的符号。那么我们有理由猜测这个符号代表的是 q，而其他三个符号表示 u。密文中其他的字母很难被确定，但也可以根据他们彼此之间的关系慢慢破译出来。虽然同音密码是可以破解的，但它比直接的单字母密码安全得多。

表 5：一个同音替换密码的例子。最上面一行是明码字母表，下面的数字表示的是常用字母选择的密码字母表。

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
09	48	13	01	14	10	06	23	32	15	04	26	22	18	00	38	94	29	11	17	08	34	60	28	21	02
12	81	41	03	16	31	25	39	70			37	27	58	05	95		35	19	20	61		89		52	
33		62	45	24			50	73			51		59	07			40	36	30	63					
47			79	44			56	83			84		66	54			42	76	43						
53				46			65	88					71	72			77	86	49						
67				55			68	93					91	90			80	96	69						
78				57										99					75						
92				64															85						
				74															97						
				82																					
				87																					
				98																					

同音密码看上去似乎跟多字母替换密码相似，因为每个明文字母有多种加密选择。但是它们有一个关键的区别，同音密码事实上是一种单字母密码。在上面所示的同音表中，字母 a 可以表示成 8 个数字。但重要的是，这 8 个数字只代表一个字母 a。换句话说，一个明文字母可以表示成多个符号，但每个符号只能表示一个字母。在多字母密码中，明文字母也可以表示成多个符号，但

是更复杂的是在一次加密过程中代表不同的字母。

同音密码被认为是单字母密码的根本原因或许是这样的：一旦密码表被确定，那么在整个加密过程中它是保持不变的，尽管每个字母有几个加密选择。但是，在加密过程中，一个密码编码师在使用多字母替换密码时必须不断地在不同的密码表之间来回替换。

在单字母替换密码的基础上，我们可以进行各种各样小的改进。例如引入同音字，就有可能提高加密的安全性，并且没有多字母密码那么复杂。在各种改进的单字母密码中，最著名的一个例子是路易十四的大密码，大密码用来加密国王最机密的信息，保护他的政治计划。其中一个信息就提到了法国历史上最神秘的人物——铁面人。但是由于大密码的安全，导致这个信息和其中令人称谓的内容两个世纪来都无法被破译。大密码是由一对父子发明的。父亲安东尼·罗西格诺和儿子博纳凡托·罗西格诺，安东尼第一次成名是在1626年，当时法国正包围雷阿勒蒙，有个信使带着一封加密的信件从该城市逃出来但被捕获。这封加密信件就交给了安东尼破译，当晚他就破解了这封信，信中揭示防守这座城的于格诺军队已经濒临崩溃的边缘。法国人先前并没有认识到于格诺的绝望处境，便送回了这封信并在后面附上解密后的内容。于格诺这次知道他们的敌人不会退兵便立即投降了。这次解密使法国没费一枪一弹就取得了胜利。密码破解的威力是显而易见的，罗西格诺父子很快在宫廷里有了高级职位。他们先为路易十三效劳，接着又做为路易十四的密码破译师。路易十四对密码看得是如此的重要，以至于他将父子俩的办公室移到他的住处旁边，这样他们就可以在法国外交政策的形成过程中扮演一个中心角色。对他们能力一个最好的说明就是由他们名字形成的单词成为法国人的一个俚语，这是用来表示撬锁的一种装置，意在影射他们破解密码的能力。

罗西格诺在破解密码的同时也在考虑如何创造一种更强大的加密方法，于是他们发明了所谓的大密码。大密码是如此的安全，以至于敌方密码破译师对任何破解的法国密码的努力都是徒劳的。遗憾的是，在这父子俩去世后，大密码也就停止了使用，它的具体细节也很快失传，这意味着法国文档里的加密文件不能再被读懂。事实上大密码保密性非常强，它使随后几代密码破解者的努力都付诸东流。

历史学家知道这些加密的文件能使人对17世纪法国的传奇故事有独特的理解，但是直到19世纪末，他们仍不能破译它们。1890年，一位军事历史学家维克托·吉东在研究路易十四领导过的战役时，发掘出了一批新的由大密码加密的信件。由于不能看懂其中的意思，他把这些信件交给了司令官埃提恩尼·巴泽利斯，法国军事密码机构里的一位著名的专家。巴泽利斯把这些信件看成是一生中最大的挑战，他花了三年的时间来破译它们。

这些加密的文件含有成千的数字，但实际上不同数字只有587个。显然大密码比一个直接的单字母替换密码复杂得多，因为单字母密码只需26个不同的数字，每个字母一个。最初巴泽利斯认为这些数字可能代表同音，即几个数字表示一个字母。为了探索这个方法他进行了几个月的艰苦工作，却毫无结果。大密码不是一个同音替换的密码。

接下来，他突然有了个想法，那就是每个数字代表一对字母，或者说连字。总共只有26个字母，但是组成对之后就有676个连字，这大致等于密文中出现的不同的数字量。巴泽利斯假定密文中频率最高的数字(22,42,124,125,341)代表常见的法语连字(es,en,ou,de,nt)，然后他对这些双字母进行频度分析。遗憾的是，经过几个月的工作，这个理论仍没有产生任何有意义的解密结果。

再次失败之后，巴泽利斯差点放弃了他的想法。可是他最终

没有放弃,他想或许连字的想法离事实已经不远。他开始考虑另一种可能性,每个数字代表的不是一对字母,而是一个音节。最常见的数字可能代表法语中最常见的音节。他尝试了许多次但只得到一些无意义的片断。然而他最终确定了一个单词。一组在某页出现多次的数字(124 - 22 - 125 - 46 - 345)经过巴泽利斯的分析被认为是代表 les - en - ne - mi - s,这是"les ennemis"(敌人)。这显然是个关键的突破。

巴泽利斯然后继续检查密文中其他出现这些数字的部分。他把从"les ennemis"中衍生出的音节插到密文中,就揭示了其他单词的一部分。玩过填单词游戏的人知道,当一个单词部分被完成的时候,通常可以猜出另一部分。随着巴泽利斯完成一个新的单词,他又可以确定更多的音节,这些音节又可以推出其他的单词等等。他也经常被难住,有时音节永远也判定不出来,有时是因为一些数字代表的是单个字母而不是音节,也有时因为罗西格诺父子在密码留下了的陷阱。例如,一个数字既不代表一个音节,也不代表一个字母,它的存在仅仅是用来删除前面一个数字。

当解密完成的时候,巴泽利斯成了两百年来第一个见证路易十四秘密的人。这些新解密的材料极大地迷住了历史学家,他们都将焦点放到了一封信上。它似乎解决了 17 世纪最大的谜团之——铁面人的真实身份。

自从铁面人第一次被囚禁在法国萨瓦的皮尼罗尔城堡之后,关于他的猜测就一直没有断过。1698 年,当他被转移到巴斯蒂勒的时候,仆人试图偷看了他一眼,从此关于他是高是瘦,是白是胖,以及年龄大小的各种说法都被传遍开来。有时甚至有人说他是个女的。由于不知道事实究竟是怎样,从维奥泰尔到本杰明·富兰克林的每一个人都有自己一套关于铁面人的理论。和铁面人有关的最流传的一个猜测就是他是路易十四的孪生兄弟,他被囚禁起来以免引起争论,即究竟谁是合适的王位继承者。这个理论的一个

说法是这个铁面人存在后裔，他们含有不为人知的皇家血统。1801年曾出版一个小册子说拿破仑本身就是铁面人的后代。关于这个传言，拿破仑在巩固了他的位置之后并没有否认它。

由于铁面人的神秘，甚至出现了诗词、散文和戏剧来描述它。1848年维克托·雷格开始写一部名为《双胞胎》的剧本，但当他发现大仲马已经写过同样的情节后，他放弃了。从那以后，人们就将大仲马的名字和铁面人的故事联系在一起。他小说的成功更加强了铁面人与国王之间关系的猜测。虽然巴泽利斯的解密揭示了事实的真相，但是这个理论已经深深印人人们脑海中了。

巴泽利斯已经解密了由路易十四的首相弗朗索瓦·德·卢瓦写的一封信。其中先说明了菲芬·德·布洛德的罪行，他曾是一位司令官，负责领导攻击法国和意大利边界库内奥城镇。尽管他被命令防守自己的领地，但布洛德非常害怕敌人从奥地利进攻，于是他逃跑了，留下了军需品并抛弃了许多受伤的士兵。根据首相的说法，这次行动危及整个皮埃蒙特区战役，这封信很显然表明国王将布洛德的行动视为极端怯懦的行为。

> 国王陛下比任何一个人都明白这次行动的后果，他也认识到我们的失败多么严重地损害了我们的利益，必须在冬天有所弥补。陛下希望你立刻逮捕布洛德将军，并送到皮尼罗尔城堡接受审判，在那儿他晚上要被关押在牢狱里，白天可以允许戴着面具在城墙内走动。

这里明确地提到了皮尼罗尔的戴面罩的人，一个足够严重的罪行，时间也和铁面人传说吻合。这是否就解开了那个谜团？不奇怪，那些赞成更传奇说法的人也发现了布洛德说法的不符。例如，有一种辩解是，如果路易十四真的试图秘密囚禁他不愿承认的双胞胎弟弟，那他将会留下一系列的假象。或许这个加密的信件

就是希望能被解密,或许 19 世纪的密码破解者巴泽利斯已经钻进了 17 世纪编码人所设的一个圈套。

密室

17 世纪引入的音节和同音字加强了单字母密码,这似乎已经足够了。但是到了 18 世纪,密码破译术已是相当盛行,通常是政府的几组密码破译者一起工作,他们破解了许多最复杂的单字母替换秘码。每个欧洲政权都拥有自己的密室——破解密码和收集情报的中枢。最有名的、也最有组织和效率的密室是维也纳的勘兹雷。

密室严格地按照时间来运作,因为这种隐秘的地下活动是万万不能阻碍邮政系统的正常运行的。凡是发送给驻维也纳大使的信件早晨七点先被送到密室,由助理先去封印,然后一批文学家分工拷贝信件,必要时候,语言专家负责复制一些不寻常的手迹。三小时后信件重新封印到信封里,再发送到邮政中心,那里信件将被送往目的地。上午十点左右发往奥地利本国内的信件被送到密室,而由驻维也纳大使发往到奥地利以外的信件下午四点到达密室。所有的信件在发送过程中都被拷贝。每天经维也纳密室过滤的信件有一百多封。

信件拷贝后被送到密码破译者手中,他们通常坐在特别的小屋里,时刻准备着破解这些信息。维也纳密室除了向奥地利皇帝提供有价值的情报外,他们也把收集到的信息卖给欧洲其他国家。1774 年他们和法国驻维也纳使馆的秘书阿博特·若热尔达成一笔交易,他们向阿博特·若热尔提供了一些信息,代价是 1000 达克特。阿博特·若热尔即刻发信给巴黎的路易十五,报告了其他一些君主可能的秘密计划。

事实上，密室使所有的单字母替换密码都不再安全，在这些专业的密码破译家面前，密码编码家最终不得不采纳更复杂并且更安全的维热纳尔密码。密码助理们逐渐地开始改用多字母替换密码。这种转换一方面是因为迫于密码破译术的压力，而另一方面则是因为电报的发展，需要保护电文不被截获和破解。

虽然19世纪出现的电报是电信革命的一个产物，但它的原型则可追溯到1753年。苏格兰杂志上有篇匿名文章描述了通过用26个线缆将发送方和接收方连接起来，可以进行远距离的发送信息，其中每根线缆代表字母表中的一个字母。发送者通过向每根线缆施加电脉冲来发出信息。例如要发送hello，发送方先沿着h线发送一个信号，再沿着e线发送，依次下去。接收方则通过感觉每根线缆上的电流变化来读出信息。然而，因为一些技术上必须克服的困难，这个被发明者称为“传播情报的快速方法”最终没有被建成。

例如工程师需要一个非常敏感的系统来检测电信号。英国的查利斯·惠特斯通和威廉姆·福瑟吉尔·库克用磁化的针头制成检测器，当有电流来的时候，它将发生偏转。1839年，惠特斯通－库克系统被用来在西德雷顿和帕丁顿的两个铁路车站之间传送信息，距离为29公里。从此，电报的名声以及它那令人吃惊的传送速度迅速被传遍开来。

而最能显示出电报威力的一个例子莫过于1844年8月6日维多利亚女王第二个儿子——阿尔弗莱德王子的出世。出生的消息通过电报传到伦敦，一小时后街上的《时代》杂志就已宣布这条消息，并特别赞颂了这项技术，它提到这一切都“归功于电报非同寻常的威力”。第二年，借助电报警察抓获了罪犯约翰·托厄尔，他谋害了他的妻子，跳上一辆去往伦敦的火车企图逃跑，地方警察将托厄尔的描述通过电报传到伦敦，他一下火车就被捕了。这样电报的名声更加显赫。

而与此同时,美国的塞缪尔·莫尔斯也建成了第一个电报线路,从巴尔的摩到华盛顿跨越 60 公里。莫尔斯使用一块电磁铁来加强信号,使得信号到达接收端后还十分强烈地在一张纸上作出一系列或短或长的点或短横。他也发展了现在熟悉的莫尔斯电码,将 26 个字母译成一系列的点和短横,如表 6 所示。他还设计了一个发声器,接收方能够根据一系列发声的点和短横直接听出每个字母。

回到欧洲,莫尔斯的密码逐渐代替了惠特斯通 - 库克系统。1851 年,整个欧洲大陆采用了莫尔斯电码的欧洲版本,其中包括了一些地方化的字母。随着时间的推移,莫尔斯密码和电报对这个世界的影响也越来越深:警察抓到更多的罪犯;报纸有了及时的消息;为商业活动及时提供了有价值的信息;远距离的公司能够作出及时的反应等。

然而,如何保护这些通常是敏感内容的通讯却是个大问题。莫尔斯电码本身并不是某种形式的密码,因为对信息而言没有任何隐藏。点和短横仅仅是用来表示字母的一种便捷方法。莫尔斯电码事实上就是另一种形式的字母表。安全问题变得首要突出,因为任何想发送信息的人都不得不将信息发给莫尔斯电码操作员,操作员再读出并翻译出来。如果电报员能知道任何的信息,那么这就存在一个危险:一个公司只要贿赂一个操作员,那样就完全取得了对手的通讯资料。

1853 年,英国杂志《每季回顾》登了一篇有关电报的文章,其中就讲述了这个问题。

> 应该采取有效手段来消除电报发送私人信息的一个大缺陷——秘密荡然无存,因为无论如何都会有五、六个人知道一个人向另一个人传送的秘密。英国电报公司的雇员都发誓保守秘密,但我们通常不能容忍陌生人在我

们的面前读着我们写的东西。这是电报的一个令人难解的不足，它必须通过一些手段来弥补。

表 6:国际莫尔斯电码符号

Symbol	Code	Symbol	Code
A	·-	W	·--
B	-···	X	-··-
C	-·-·	Y	-·--
D	-··	Z	--··
E	·	0	-----
F	··-·	1	·----
G	--·	2	··---
H	····	3	···--
I	··	4	····-
J	·---	5	·····
K	-·-	6	-····
L	·-··	7	--···
M	--	8	---··
N	-·	9	----·
O	---	full stop	·-·-·-
P	·--·	comma	--··--
Q	--·-	question mark	··--··
R	·-·	colon	---···
S	···	semicolon	-·-·-·
T	-	hyphen	-····-
U	··-	slash	-··-·
V	···-	quotation mark	·-··-·

解决方法就是在将信息递给电报员之前对信息加密,电报员在传送之前将密文变成莫尔斯电码。加密除了防止电报员看到敏感的资料外,也能使那些窃听电波线路的间谍白白辛苦一场。多字母替换密码显然是用来加密重要的商业通讯的最好方法。它被认为是无法破解的,密码编码者至少有一次领先于密码破译家了。

巴比奇破解维热纳尔密码

19世纪密码破译术中最让人感兴趣的人物是查尔斯·巴比奇,一个性情古怪的天才,他最著名的成就是建立了现代计算机的理论框架。巴比奇生于1791年,父亲本杰明·巴比奇是个富裕的银行家。当他没有征得父亲同意结婚后,就被剥夺了继承权。但他仍有足够的钱来保障生计,他追求一种无拘束的学者生活,解决任何他感兴趣的问题。他的发明包括速度计和排障器——一种装在蒸汽火车前部用于清除铁轨上障碍的装置。在科学上,他第一个认识到树的年轮的宽度与当年的气候有密切联系,他提出通过研究古代的树木可能会得出过去的气候。他也对统计学产生过兴趣,作为消遣,他画了一套死亡率统计表,直到今天仍作为保险业的一个基本工具。

巴比奇没有把自己限制在解决科学和工程问题上。当时,发送一封信件的费用根据信件传送的距离确定,而巴比奇指出仅用来计算每封信价格所需的劳力费用就比邮费本身都高。他提出了所有信件单一价格系统,不管邮件发往国家哪个地方,至今我们仍在延用。

他也对政治和社会感兴趣,在他生活晚年,他领导了一项运动,志在除去漫游在伦敦街头的风琴师和卖唱者。他抱怨街边音乐几乎会毫无例外地形成一个舞场,都是一些穿着破烂的小顽童,

有时是半醉半醒的男人，偶尔他们会用一些不协调的噪音来附和那些噪音。

而街边音乐却有一群极大的支持者们，一般由女士组成。她们对道德观没有看得很重，有四海为家的倾向。对她们来说街边音乐为她们能够公开表露自己的爱好，提供了一个文明的理由。不幸的是，歌唱者们聚集了一大群人在巴比奇的住处周围，并尽可能大声地演唱。

巴比奇科学生涯的转折点是在1821年，当时他和天文学家约翰·赫舍尔在检查一组数学表。这是天文学、工程学和航海学计算中常用的一个基础表，无奈表中含有诸多的错误，这些错误反过来导致一些重要的计算结果无效。其中一组表是用于在海上决定经纬度的航海星历表，含有一千多处错误。事实上，许多海难和工程事故都归咎于错误的数表。这些数学表是由手工计算的，其错误也只是人为的结果。这使得巴比奇声称："我希望这些计算能够向蒸汽火车那样自动进行。"这标志着一项非凡举措的开始，即建造一台能够高标准地计算这些数表的机器。1823年，巴比奇设计了"差分机1号"，这台由2500个精位组成的计算器在政府的资助下建成。尽管巴比奇是个天才的改革者，但他却不是伟大的改进者。经过十年的艰辛之后，他放弃了"差分机1号"，开始了一个完全新的设计，着手建造"差分机2号"。

当巴比奇决定放弃"差分机1号"后，政府对他失去了信心，为了减少损失决定从该项目撤资，要知道该计划已经花费了17470英镑，这足以建造两艘战船。可能正是这次经济支持的取消导致巴比奇后来抱怨："如果你向一个英国人介绍一种原理和一种仪器，无论它是多么的美妙，你会发觉英国式思想最终是要发现其中的困难度、缺陷或者干脆是它的不可能性。如果你对他口述一种能够削土豆皮的机器，他会声明这是不可能的；如果你在他面前用该机器削土豆皮，他会表示这根本无用，因为它不会削菠萝。"

政府投资的短缺意味着巴比奇永远不能完成他的“差分机 2 号”。这是科学史上的一个悲剧，因为巴比奇的机器不仅可以用来计算特定的一些数据表，它本来还可以发展为以后的解析机。



图 12：查尔斯·巴比奇。

在巴比奇自己的一生中,除了差分机以外,他在密码破解上同样也做出了一次重要的贡献:他成功地破解了维热纳尔密码。这样的话,他就完成了一次自9世纪阿拉伯学者提出频度分析破解单字母替换密码以来,在密码破译学史上最伟大的突破。巴比奇的工作不需要任何复杂的计算,他采用的纯粹是技巧。

巴比奇在非常年轻的时候就对密码产生了兴趣。他后来回忆童年时代的兴趣怎样使他陷入麻烦:"大孩子经常作密码,可是我一旦找到一些单词,一般就会发现它们的密钥,这种小聪明的结果有时是很痛苦的,那些密码有时被人察觉会招来痛打,这都是因为他们的愚蠢。"可是挨揍并没有使他气馁,他仍然着迷于密码破译。他在自传中写道:"我认为破解密码是最迷人的事情。"

他很快在伦敦有了名气,作为一个密码破译师他准备着破解任何被加密的信息,陌生人可以带着各种问题来找他。例如他曾帮助一个几乎绝望的传记作者破解了英国第一位皇家天文学家约翰·弗拉姆斯蒂德的速记笔记。他也协助一位历史学家解决了查尔斯一世夫人玛利亚的一个密码。1854年,他和一位律师联手,使用密码破译揭露出一件大案中的一个关键证据。在那几年里,他积累了厚厚一堆加密的信息,他准备在这基础上写一本关于密码破译的权威著作,名为《密码破解哲学》。这本书预先计划对每种密码介绍两个例子:一个将用于讲解破译密码的方法,另一个则留给读者作为练习。很遗憾,和他的其他的许多伟大计划一样,这本书最终也未完成。

当大多数密码破译师已经放弃了破解维热纳尔密码的任何希望的时候,巴比奇正试图破解这个密码。事情缘起布里斯托尔的一个牙医约翰·布罗克·赛瓦特。这个牙医其实对密码了解相当少,1854年他声称他已发明了一个新密码,实际上就相当于维热纳尔密码。他写信给《艺术协会杂志》想给他的发现取得专利,显然他没有想到他已经迟了几个世纪了。巴比奇写信给协会指出

“密码……很早就有，可以在很多书中找到”。赛瓦特却不愿承认，并为难巴比奇让他破解这个密码。其实密码能否破解与密码是不是新的没有关系，可这已经足以激起巴比奇的好奇心去寻找维热纳尔密码的弱点。

破解一个困难的密码就像爬一座陡峭的崖壁。密码破译家要一直寻找任何凹处和裂缝来作为立足点。在单字母替换密码中，密码破译家需要了解各个字母的频率，因为最常见的字母如 e、t 和 a 无论怎么隐藏都会露出马脚。但对于多字母维热纳尔密码，字母的频率被很大程度上平衡了，因为使用了关键词来替换密码表。所以，乍看上去，岩石表面似乎相当光滑。

记住，维热纳尔密码的长处在于同样的字母以不同的方式被加密了。例如，如果关键词是 KING(国王)，那么明文中每个字母潜在地可以通过 4 个途径加密，因为关键词中有 4 个字母。关键词中的每个字母定义了维热纳尔方阵(表 7)中的一个不同密码字母表，方阵中的 e 列被加黑，以表明根据关键词中的哪个字母的定义，e 是如何被不同地加密的。如表下：

如果 KING 中的 K 用来加密 e，那么结果密文中的字母是 O。
如果 KING 中的 I 用来加密 e，那么结果密文中的字母是 M。
如果 KING 中的 N 用来加密 e，那么结果密文中的字母是 R。
如果 KING 中的 G 用来加密 e，那么结果密文中的字母是 K。

同样，一个单词也可以用 4 种方式来加密。例如，单词 THE，根据它与关键词的相对位置，可被加密成 DPR、BUK、GNO 和 ZRM。尽管这使得密码破译很困难，但也不是不可能。重要的一点在于有 4 种方法用来加密单词 the，而在原始信息中 4 次以上出现了单词 the，那么就存在很大的可能性，即在密文中这 4 种可能的加密方法出现了重复。我们以下面的例子来说明一下，例中明

文 The Sun and the Man in the Moon("在月亮中的太阳与人")已用维热纳尔密码和关键词 KING 加密。

表 7:维热纳尔方阵与 KING 相结合。关键字被定义为 4 个不同的密码字母表,所以字母 e 可被加密为 D,M,R 或 K。

Plain	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	[illegible]	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	[illegible]	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	[illegible]	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	[illegible]	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	[illegible]	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
[illegible]	[illegible]	[illegible]	[illegible]	J	K	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
7	H	I	J	K	[illegible]	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
[illegible]	[illegible]	[illegible]	K	L	M	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
9	J	K	L	M	[illegible]	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	O	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
11	L	M	N	O	[illegible]	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	[illegible]	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
[illegible]	[illegible]	[illegible]	[illegible]	Q	R	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
14	O	P	Q	R	[illegible]	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	[illegible]	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	[illegible]	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	[illegible]	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	[illegible]	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	[illegible]	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	[illegible]	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	[illegible]	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	[illegible]	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	[illegible]	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	[illegible]	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	[illegible]	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	[illegible]	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

关键词 K I N G K I N G K I N G K I N G K I N G K I N G

明　文 t h e s u n a n d t h e m a n i n t h e m o o n

密　文 D P R Y E V N T N B U K W I A O X B U K W W B T

第一个单词 the 被加密成 DPR,第二和第三个 the 被加密成 BUK。出现 BUK 重复的原因是第二个 the 和第三个 the 相差 8 个位置,8 是关键词长度 4 的整数倍。换句话说,第二个 the 根据它与关键词的关系(the 在 ING 的下方)先进行了加密,等我们到达第三个 the 的时候,关键词正好轮回了两次,即重复了这种关系,因而也重复了同样的加密。

巴比奇认识到这种重复正为他提供了征服维热纳尔密码所需的一个立足点。他建立了一系列的步骤,任何密码破译者可以遵循它来破解当时无法破解的维热纳尔密码。为了说明这项卓越的技术,让我们想像我们已经截获如图 13 所示的一个密文,假定我们知道它是用维热纳尔密码加了密,但我们不知原文究竟是什么,关键词也是个迷。

巴比奇密码破译的第一步是寻找密文中出现超过一次的字母串,有两种情况可能导致这样的重复发生。最有可能的是明文中同样的字母序列使用密钥中同样的字母加了密。另外还有一种较小的可能性是明文中两个不同的字母序列通过密钥中不同部分加了密,碰巧都变成了密文中完全一样的序列。假如我们限制在长序列范围内,那么第二种可能性可以很大程度地被排除,这种情况下,我们将考虑到 4 个字母或 4 个以上的重复序列。表 8 是这样重复序列的一个记录,其中也表示出每种重复序列之间间隔的字母数。例如序列 E－F－I－Q 出现在密文中的第一行和第九行,中间隔了 95 个字母。

关键词除了用来将明文加密成密文外,接收者也要用它来将密文解密成明文。因此,如果我们确定了关键词,解密将是很容易的。到目前为止,我们还没有足够的信息来找出关键词。但表 8 却为关键词的长度提供了一些非常好的线索。表 8 中除了列出了哪个序列发生重复以及每个重复序列之间的间隔,其余部分则给出了间隔包含的“因子”。例如序列 W－C－X－Y－M 在 20 个字

母之后重复了一次，那么数字 1、2、4、5、10 以及 20 就是“因子”，因为它们能够整除 20。这些因子表明了 6 种可能性：

```
WUBEFIQLZURMVOFEHMYMWT
IXCGTMPIFKRZUPMVOIRQMM
WOZMPULMBNYVQQQMVMVJLE
YMHFEFNZPSDLPPSDLPEVQM
WCXYMDAVQEEFIQCAYTQOWC
XYMWMSEMEFCFWYEYQETRLI
QYCGMTWCWFBSMYFPLRXTQY
EEXMRULUKSGWFPTLRQAERL
UVPMVYQYCXTWFQLMTELSFJ
PQEHMOZCIWCIWFPZSLMAEZ
IQVLQMZVPPXAWCSMZMORVG
VVQSZETRLQZPBJAZVQIYXE
WWOICCGDWHQMMVOWSGNTJP
FPPAYBIYBJUTWRLQKLLLMD
PYVACDCFQNZPIFPPKSDVPT
IDGXMQQVEBMQALKEZMGCVK
UZKIZBZLIUAMMVZ
```

图 13：用维热纳尔密码加密的密文。

(1) 密钥是 1 个字母，两次加密之间重复了 20 次。
(2) 密钥是 2 个字母，两次加密之间重复了 10 次。
(3) 密钥是 4 个字母，两次加密之间重复了 5 次。
(4) 密钥是 5 个字母，两次加密之间重复了 4 次。
(5) 密钥是 10 个字母，两次加密之间重复了 2 次。
(6) 密钥是 20 个字母，两次加密之间重复了 1 次。

第一种可能性可以被排除，因为只有一个字母的密钥实际就成了单字母替换密码，维热纳尔方阵中只有一行用来整篇加密，密码表保持不变，一个密码编码师不可能这样做。表 8 中我们使用√号来表明每一个其他的可能性，每个√号即表示一个可能的密钥长度。

为了确定密钥究竟是2个、4个、5个、10个还是20个字母长度，我们需要查看其他所有间隔的因子。因为关键词似乎应小于20个字母，因此表8仅列出了每个间隔20及20以下的因子。从表中可以明显地看出这些间隔都有能被5整除的倾向。事实上，每个间隔都能被5整除。对于第一个重复序列E-F-I-Q，我们可以认为，从其第一次加密到第二次加密，长度为5的关键词轮回了19次。对第二个重复序列P-S-D-L-P，从第一次加密到第二次加密，长度为5的关键词仅轮回了1次。第三个重复序列W-C-X-Y-M两次加密间，长度为5的关键词轮回了4次。第四个重复序列E-T-R-L两次加密间，长度为5的关键词轮回了24次。简言之，每个重复序列都与5字母的关键词有关。

表8：密文中的重复和字间距。

重复序列	重复间隔	密钥的可能长度																		
		2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
E-F-I-Q	95				✓														✓	
P-S-D-L-P	5				✓															
W-C-X-Y-M	20	✓		✓	✓					✓										✓
E-T-R-L	120	✓	✓	✓	✓	✓		✓		✓		✓			✓					✓

假定关键词真的是5个字母长度，下一步即要解决关键词的实际字母。暂且我们将关键词表示成L1-L2-L3-L4-L5，其中L1表示关键词的第一个字母，依此类推。加密过程的第一步是根据关键词的第一个字母L1，加密明文的第一个字母。字母L1代表了维热纳尔方阵的一行，也就是为明文中的第一个字母提供了一个单字母替换密码表。而当加密进行到明文第二个字母时，密码编码师将使用L2来代表维热纳尔方阵中的一个不同的

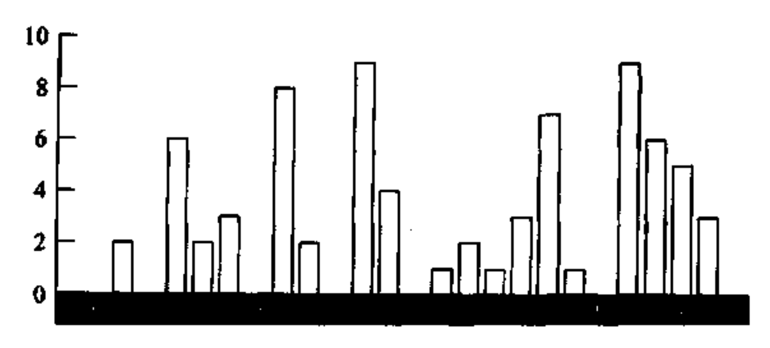


图 14:以 L1 密码字母表加密的密文的字母频率分布。

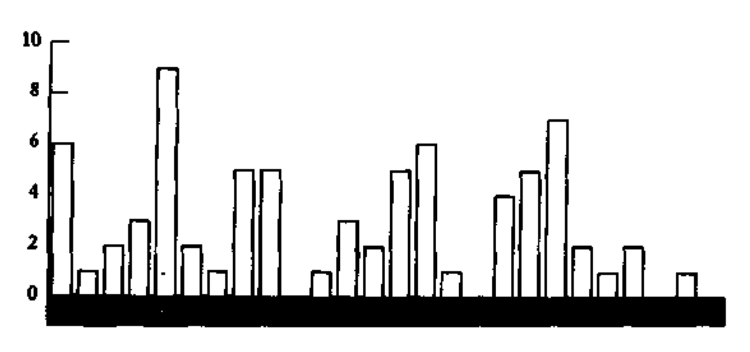


图 15:标准的频率分布。(明文与密文中的字母数量相同)

行,也即提供了一个不同的单字母替换密码表。明文第三个字母将根据 L3 来加密,第四个字母根据 L4,第五个字母根据 L5。关键词中的每个字母为加密提供了一个不同的密码表。但是,明文中第六个字母将再次根据 L1 来加密,第七个字母也再次根据 L2 来加密,这种轮回就这样重复下去。换句话说,多字母替换密码是由 5 个单字母替换密码组成,每个单字母替换密码负责加密 1/5 的明文,而更重要的是,我们已经知道如何去分析单字母替换密码。

我们按如下方法来进行,我们知道维热纳尔方阵中由 L1 决

定的那一行为加密明文中第1、第6、第11、第16个等等字母提供了密码表。因此，我们如果只看密文中的第1、第6、第11、第16个等字母，我们将能够使用古老的频度分析来确定出其所用的密码表。

图14显示了密文中第1、6、11、16……字母的频率分布，它们是W、I、T、E……。在这里我们须记住维热纳尔方阵中的每个密码字母表与标准字母表相比仅仅是交错了一定位数，其值是从1到26位。因此图14中的频率分布应和一个标准字母表的频率分布有相似的特性，它们之间区别在于相互错开了一些位置。通过比较L1分布和标准分布，将有可能得出它们的移位数。图15表示了由一篇英文明文得出的一个标准频率分布。

标准频率有峰值、平稳期和谷。将它和L1密码分布相匹配，寻找两者之间最显著的相似特性。例如在标准分布中R-S-T处有三个峰值(图15)，在其右面从U到Z六个字母则形成一段低谷期，这是一个比较突出的现象。在L1分布中惟一与此相似的现象(图14)是在V-W-X处有三个峰值，后面接着从Y到D六个字母的低谷期。这似乎暗示着所有根据L1来加密的字母都移动了4个位置，或者说，L1决定的密码表是从E、F、G、H……开始的。反过来这意味着关键词第一个字母L1可能是E。我们可以检验一下这个假设，将L1分布往回移动4个位置，再将它与标准分布相比。图16显示了这两个分布，从中可以看出几个主要峰值之间的吻合恰到好处，表明我们可以安全地认为关键词确实从E开始。

现在我们来概括一下以上过程：寻找密文中的重复序列以确定关键词的长度，结果发现有5个字母，这使我们将密文分成5个部分。每个部分都根据一个单字母替换密码来加密。通过分析密文中由关键词第一个字母加密的部分，我们能够得出字母L1可能是E。重复这样的过程来确定关键词的第二个字母，根据密文中第2、7、12、17……字母建立频率分布，结果见图17，将它与标准

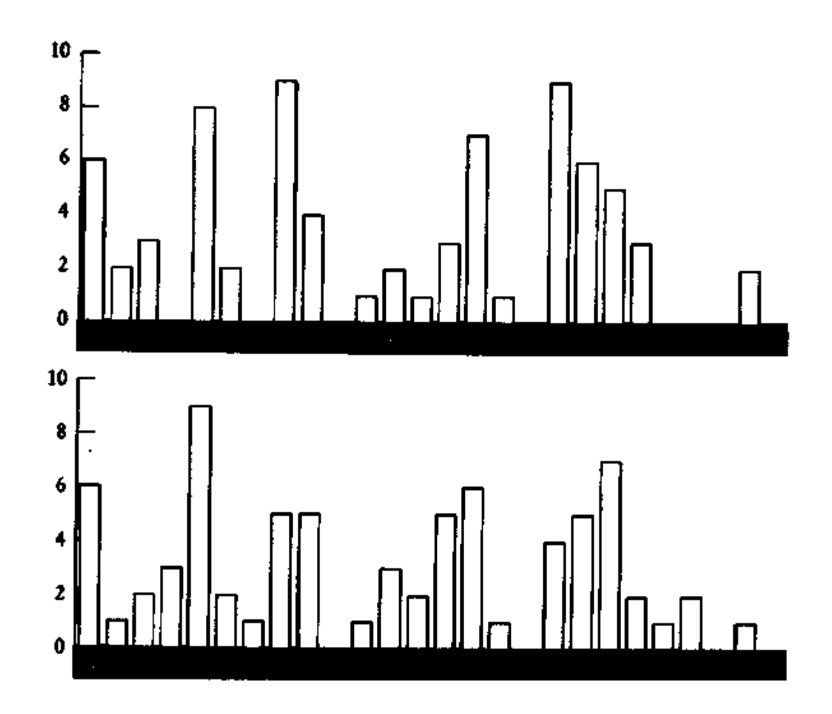


图 16:L1 分布后移 4 个字母(上图),与标准频率分布相比较(下图)。所有主峰和凹处相配合

分布再次比较以推出移位数。

这个分布相对较难分析。没有明显的三个相邻峰与标准分布的 R－S－T 相对应。然而其中从 G 到 L 的一段低谷期却很明显,这很可能与标准分布中从 U 到 Z 的那段相对应。如果是这样,我们就认为 L2 分布中的 D、E、F 相当于标准分布中的 R、S、T,但是在 E 处没有峰。暂时我们把这个丢失的峰作为一个统计误差,继续我们最初的发现,即从 G 到 L 的低谷期是个明显的移位特征。这表明所有根据 L2 加密的字母已被移动了 12 个位置,或者说 L2 决定的密码表是从 M、N、O、P……开始,关键词第二个

字母 L2 是 M。我们可以再次通过将 L2 分布回移 12 个位置后与标准分布作比较来检验这个推测。图 18 显示了这两个分布，其主要的峰值很好地吻合在一起，表明我们可以放心地断定关键词第二个字母确实是 M。

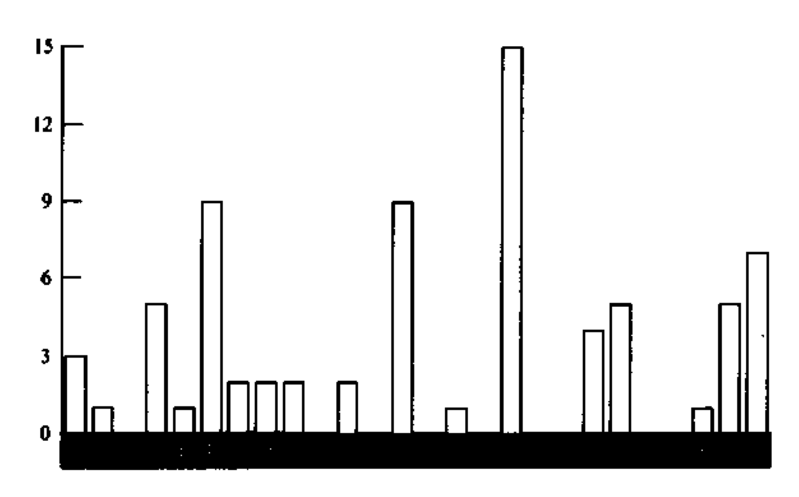
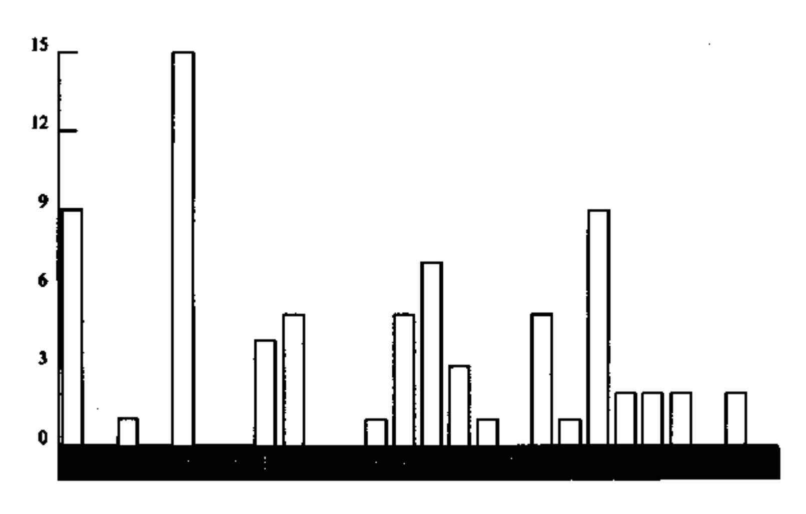


图 17：利用 L2 密码字母表得到的密文中字母频率分布图。

我不再继续分析下去，只告诉大家分析密文字母第 3、8、13……可以得出关键词第三个字母是 I，分析字母第 4、9、14……表明关键词第四个字母是 L，分析字母第 5、10、15……发现关键词第五个字母为 Y，关键词是 EMILY。现在就可以逆转维热纳尔密码，完成密码破译了。密文第一个字母是 W，它是根据关键词第一个字母 E 来加密的。回过头看维热纳尔方阵，找到方阵中 E 行 W 列，发现这列最顶端字母是 S，这必定是明文中的第一个字母。重复这样的过程，我们发现明文是 sittheedownandhavenoshamecheekbyjowl……



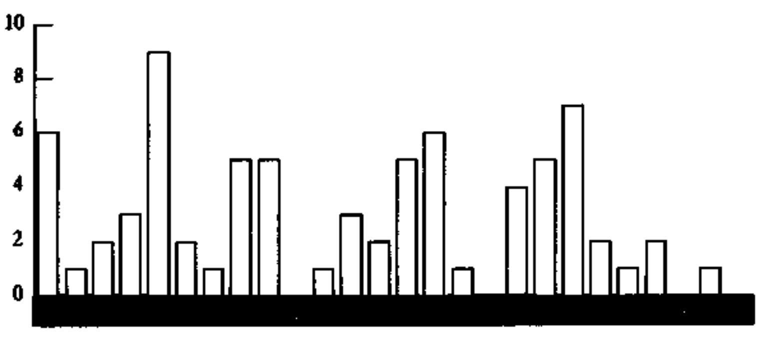


图 18:将 L2 分布回移 12 个位置(上图),与标准分布作比较(下图)。

插入合适的空格和标点,我们最终得到:

Sit thee down, and have no shame,	请你坐下,不要害羞,
Cheek by jowl, and knee by knee:	面对面,膝对膝:
What care I for any name?	有什么名字会使我关心?
What for order or degree?	有什么秩序会使我着迷?

Let me screw thee up a peg:	让我为你拧上一颗螺钉:
Let me loose thy tongue with wine:	让我把你灌醉:
Callist thou that thing a leg?	你把那东西叫腿吗?
Which is thinnest? Thine or mine?	哪一只最细? 是你的还是我的?
Thou shalt not be saved by works:	你不该被拯救:
Thou hast been a sinner too:	你已经成为一个罪人:
Ruined trunks on withered forks,	破烂的树干在枯萎的耙子上,
Empty scarecrows, I and you!	你和我都是空虚的稻草人!
Fill the cup, and fill the can:	注满酒杯,注满罐子:
Have a rouse before the morn:	在黎明到来之前快快醒来:
Every moment dies a man,	每一瞬间都有人死亡,
Every moment one is born.	每一瞬间都有人诞生。

巴比奇可能是在1854年成功地破解了维热纳尔密码,也就是和赛瓦特争吵之后。但他的发现却完全不为人所知,因为他从未发表它。这个发现直到20世纪当学者检查巴比奇丰富的笔记时才被公布于世。而与此同时,另一个人也独立地发现了他这种技术。他就是弗里德里克·威廉·卡西斯基,普鲁士军队的一位退役军官。1863年他发表了他在密码破译学上的突破《加密和解密的艺术》,这个方法后来被称为卡西斯基测试,而巴比奇的贡献却很大程度上被忽略了。

对于这样一个重要的密码,为什么巴比奇没有发表他的破解方法呢? 他的确有一种习惯,就是没有完成的课题,他不会发表。这次或许是他这种懒洋洋态度的另一个例子罢了。然而还有另外一种解释,他的发现正好发生在克里米亚战争爆发之后,这给了英国相对于俄军的一个明显的优势。因而很可能英国情报人员要求

巴比奇对他的工作保密，从而使他们领先于世界其他地方达 9 年之久。如果真是这样，那么这符合一个国家从国家安全角度出发，对破解密码上所取得的成就采取保密的传统，这种现象一直持续到现在。

从激情栏到埋藏的宝藏

巴比奇和弗里德里克·卡西斯基的突破使得维热纳尔密码不再安全。在这场通讯战争中，密码破译者又一次夺回了控制权，而编码者不再能保障安全。尽管密码编码者试图设计新的密码，但是在 19 世纪后一半时间里一直没有重大突破，密码编码学陷入混乱状态。然而也正是这段时期普通大众对密码产生了浓厚兴趣。

电报的发展不仅激起了商人对密码编码的兴趣，也使大众对密码编码学产生浓厚兴趣。大众开始认识到有必要保护一些非常敏感的私人信息，哪怕加密将花费更多时间与费用。莫尔斯电码操作员发送标准英文每分钟可达 35 个单词，因为他们能够记住整个词组，可以瞬间发送。而密文中的字母紊乱将极大地减慢传送速度，因为操作员需要不断地回头检查发送者信息中下一个是什么字母。普通大众使用的密码虽然不能抵挡专业密码破译师的攻击，但对付一些随意的窥探者是足够了。

当人们对加密应用自如的时候，他们开始将加密技术应用到各个方面。例如在维多利亚时代，英国年轻的情侣禁止公开表白各自爱慕之心，甚至不敢互相通信，以防他们父母截住并偷看信的内容。这使得情侣之间通过报纸的个人信息专栏互相发送加密的信息。这些所谓的“激情栏”引起了许多密码破译师的好奇，他们经常搜寻这些记录试图破解出其中的感情秘密。查尔斯·巴比奇据悉就曾迷于这种活动，他和他的朋友查尔斯·惠特斯通以及巴伦

里恩·普莱费尔一起发明了一种灵巧的普莱费尔密码。有一次惠特斯通破解了《时代》上一位牛津大学学生的留言，留言中暗示他的情人与他一起私奔。几天后惠特斯通插了一句留言，用同样的密码加密，建议这对情侣不宜采取这样鲁莽的反叛行为。不久以后，杂志上出现了第三句留言，这次没有加密，是由那位女情人发来的："亲爱的查理，不要再写了，我们的密码已经被发现了。"

过了一段时期，更加多的加密留言出现在报纸上。密码编码者开始插入整段的密文，这仅仅为了挑战他们的同行。还有些时候加密的信息用来批评一些政客和组织。《时代》杂志就曾不知情地刊登了这样一句加密的话："《时代》是出版界的杰弗里斯。"它把《时代》杂志比作17世纪臭名昭著的法官杰弗里斯，暗示该杂志是无情的、欺软怕硬的出版物，充当政府的传声筒。

另一个公众熟悉使用的密码是针孔加密的广泛使用。古希腊历史学家埃涅阿斯提出一种秘密通讯的方法，先找到一篇无关紧要的文章，再在文章中一些特定的字母下面用针刺上小孔，就像在这篇文章某些字母下面有一些点一样，这些字母可以拼成一段密文，接收者很容易识别。然而如果一个外人看到这一页，他可能会忽略这难以察觉的针孔，也就忽略了其中的密文。两千年以后，英国写信的人使用了同样的方法，他们不是为了安全起见，而仅是避免过多的邮政费用。在19世纪中期邮政系统革新之前，发送一封信大约是每100英里1先令，超过大部分人的财力。然而报纸可以免费邮寄，这就使维多利亚时代节约的人们有机可乘。除了正常地写信发信外，人们开始使用针孔在一张报纸的正面拼出一段信息，然后再通过邮局发送这份报纸，不需付一分钱。

人们对密码技术的迷恋意味着密码和密文会很快进入19世纪的文学领域。在朱尔斯·维恩的《地心游记》中，对布满如尼文字的羊皮纸的解密加速了伟大旅程的第一步。这些文字只是代替密文的一部分，由它可得到一篇拉丁文的手稿，只有当字母倒转的时

候才能看见明文：当司卡塔瑞斯的影子在七月的第一天以前轻抚斯耐菲火山的时候，从火山口爬下去，勇敢地向下走，你就会到达地球的中心。"1885 年，维恩在他的小说《马塞厄斯·桑德尔夫》中也用了一篇密文作主题。在英国，阿瑟·科南·道尔爵士是最出色的密码学小说作家之一。夏洛克·福尔摩斯无庸置疑的是一个密码学专家，他曾经对华生医士说："根据一篇极小文章的主题我可以分析出 160 篇不同的密文。"福尔摩斯最著名的解密著作是《跳舞者的冒险活动》这篇密文是由一些鼓手组成的，每个姿势代表了一个不同的字母。

图 19:《跳舞者的冒险活动》中的一段密文。

在大西洋的另一边，埃德加·阿兰·波也对密码破译学产生了兴趣。他为费城的《亚历山大每周信使》写作，并向他的读者发布了一项挑战，声称他能破解任何单字母替换密码。成百的读者向他发送密文，他都成功地一一破解。虽然这只需知道频度分析，但他的读者仍为他的成就所震惊。一个崇拜他的读者宣称他是"在世界上最渊博的、最有能力的密码破译师"。

1843 年，为了充分发挥自己的兴趣，他写了一个关于密码的短故事。这篇文章广泛地被专业密码编码师颂为关于密码题材最好的小说。该故事名为《金甲虫》，讲述了威廉姆·莱格兰登的故事，他发现了一只不同寻常的金甲虫，并用路旁的一张碎纸将它包了起来。那个晚上他用包虫的那张纸画了一幅虫的图象，并拿着这张纸来到火光下看看画的是否有出人。然而他的画没了，却出现了另外一些字符。原来这些字符是用隐形墨水所写，经过刚才

火焰的一加热而显现出来。莱格兰登检查了这些字符,开始相信他手中的是通往基德船长宝藏所在地的加密地图。接下来的故事就是经典的有关频度分析的说明,从而破解了基德船长留下的线索,发现了他所埋藏的宝藏。

尽管《金甲虫》纯粹是篇幻想小说,但在19世纪确实有这么一个故事情节。故事是关于美国西部的一个牛仔,他聚集了一大批财富,有一个藏有价值2000万美元珠宝的宝藏,并写了一套神秘的密文描述了这个宝藏的地点。关于这个故事以及那些密文都包含在1885年出版的一个小册子里。尽管只有23页,但是这本小册子还是困惑了几代的密码破译师,吸引了成百的觅宝者。

故事发生在这本小册子出版前60年,从弗吉尼亚州林奇伯格市的华盛顿旅馆开始。根据小册子所说,这个旅馆和它的老板罗伯特·莫里斯是倍受人尊敬的,“他温和的脾气,正直的性格,出色的经营以及和睦的家庭很快使他名声远扬,甚至传到了其他州。”1820年,一个名叫托马斯·比尔的陌生人策马来到林奇伯格,住进了华盛顿旅馆。“从外貌上,他大概六尺高。”莫里斯回忆道,“墨黑的眼睛和头发,穿着显得比当时的服饰稍长,他的体形很对称,一看就有非同寻常的活力,但他最明显的特征是一身黝黑的皮肤,似乎经常暴露在阳光下。然而这样却并没有影响他的相貌,我认为他是我见过的最帅的人。”尽管接下来整个冬天比尔与莫里斯在一起,并且极其地受欢迎,尤其是女士,但他从未提及他的背景、他的家庭以及他到来的目的。然后在3月末,他突然地离去了,就像来时一样。

两年后的1822年1月,比尔返回了华盛顿旅馆,比以前更黑,他又一次在林奇伯格度过了冬天,春天时又消失了。但此次离去之前,他托莫里斯保管了一个锁住的铁盒子,并说里面含有“有重要价值的纸张”。莫里斯把它放进了保险柜里后便不再过问,直到

THE

BEALE PAPERS,

CONTAINING

AUTHENTIC STATEMENTS

REGARDING THE

TREASURE BURIED

IN

1819 AND 1821,

NEAR

BUFORDS, IN BEDFORD COUNTY, VIRGINIA,

AND

WHICH HAS NEVER BEEN RECOVERED.

PRICE FIFTY CENTS.

LYNCHBURG:
VIRGINIAN BOOK AND JOB PRINT,
[illegible]

图 20:《比尔手册》的第一页,这本小册子包括了我们所知道的有关比尔财宝的秘密。

有一天莫里斯收到了一封来自比尔的信，信上的日期是 1822 年 5 月 9 日，从圣路易斯寄来。在一些寒暄之后，比尔的信说明了这个盒子真正的重要性。

> 盒中含有一些文件直接关系到我和我生意伙伴的命运。如果我不在世上，它的丢失将是无法弥补的。因此你将要知道仔细看守它的必要性，千万阻止灾难的发生。如果我们当中没有人回来，那么请你在收到这封信的十年内好好地保护这个盒子。

莫里斯忠实地继续守护着这个盒子，等待比尔来取回它。但是那个神秘的皮肤黝黑的人再也没有回过林奇伯格。他消失了，再也没人见过，也没有任何解释。十年后，莫里斯是可以按照信中的指示打开这个盒子，但他似乎不愿意破坏那把锁。比尔的信曾提到 1832 年 6 月会有一张便条寄给莫里斯，估计它是来解释如何破译盒中的秘密。然而，这个便条始终未到，或许莫里斯感到如果他不能破解其中内容的话，那么则没有办法去打开这个盒子。最终在 1854 年，莫里斯的好奇心占了上风，他打开了那把锁。盒子里含有三页加密的字符和一张比尔用明文写的便条。

这个令人好奇的便条揭示了关于比尔、盒子以及密码的真相。它解释道，在 1817 年 4 月，也就是第一次与莫里斯见面的三年前，比尔和其他 20 个同伴开始了一段横穿美国的征程。当他们穿越了西部平原富裕的狩猎地带后，又来到了圣达非，在这个“小墨西哥城镇”度过冬天。3 月他们继续向北前进，沿路追踪一个庞大的野牛群，尽可能多地捕获野牛。然后，比尔提到他们开始走运了，他说：“我们队伍继续跟着野牛群，一天我们露营在一个小峡谷中，大约在圣达非以北 250 或 300 英里左右。当时我们拴好马，准备晚餐，有个人发现在岩石的一个裂缝处有些东西看上去像黄金。

其他人一看发现果真是金子,大家自然都异常兴奋。”

信中继续解释了比尔和他的伙伴在当地部落的帮助下,在以后的18个月中对金矿进行了开采,过了一段时间,他们聚集了大量的黄金,以及一些在附近发现的白银。他们也随即同意将新发现的财宝转移到一个安全的地方,并将地点定在弗吉尼亚的一个隐秘地方。1820年,比尔带着黄金和白银来到了林奇伯格,发现了一个不错的地方,把它们埋藏起来。也就是这一次他住进了华盛顿旅馆,并熟悉了莫里斯。他在那个冬末离开后,又组织了那批人继续开采那个金矿。

又一个18月后,比尔再次光顾了林奇伯格,并藏进了更多的财宝。但这次他的归来还有另外一个原因:

> 在离开我的同伴之前,我就想我们万一发生什么不幸的事,如果没有任何防备的话,我们的亲戚将得不到所埋藏的宝藏。因此告知我去挑选某个完全可信的人,如果可以找到这样的人,在万一真的有什么意外发生的情况下,这个人应该给予以信任来完成我们关于各自的愿望。

比尔认为莫里斯是那种诚实可信的人,这就是他为什么托付莫里斯这个箱子,箱子中放有三页密码纸,就是所谓的比尔密码。每一页纸上译成的密码都包含一系列数字(见表21、22和23),破译这些密码将揭示所有相关细节:第一页描述了宝藏的位置;第二页略述了宝藏的目录;第三页列出获得宝藏拥有者亲戚的名字。当莫里斯看到这些时,已经有23年没有见到托马斯·比尔了。考虑到比尔和他的伙伴可能已不在世上,莫里斯感到有义务去找到黄金并把它们分给他们的亲属。但是,因为没有许诺中的钥匙,他被迫从头开始破解密码,在余下的20年中,这个任务一直盘绕在他的心头,最后仍以失败告终。

71, 194, 38, 1701, 89, 76, 11, 83, 1629, 48, 94, 63, 132, 16, 111, 95, 84, 341, 975,
14, 40, 64, 27, 81, 139, 213, 63, 90, 1120, 8, 15, 3, 126, 2018, 40, 74, 758, 485,
604, 230, 436, 664, 582, 150, 251, 284, 308, 231, 124, 211, 486, 225, 401, 370,
11, 101, 305, 139, 189, 17, 33, 88, 208, 193, 145, 1, 94, 73, 416, 918, 263, 28, 500,
538, 356, 117, 136, 219, 27, 176, 130, 10, 460, 25, 485, 18, 436, 65, 84, 200, 283,
118, 320, 138, 36, 416, 280, 15, 71, 224, 961, 44, 16, 401, 39, 88, 61, 304, 12, 21,
24, 283, 134, 92, 63, 246, 486, 682, 7, 219, 184, 360, 780, 18, 64, 463, 474, 131,
160, 79, 73, 440, 95, 18, 64, 581, 34, 69, 128, 367, 460, 17, 81, 12, 103, 820, 62,
116, 97, 103, 862, 70, 60, 1317, 471, 540, 208, 121, 890, 346, 36, 150, 59, 568,
614, 13, 120, 63, 219, 812, 2160, 1780, 99, 35, 18, 21, 136, 872, 15, 28, 170, 88, 4,
30, 44, 112, 18, 147, 436, 195, 320, 37, 122, 113, 6, 140, 8, 120, 305, 42, 58, 461,
44, 106, 301, 13, 408, 680, 93, 86, 116, 530, 82, 568, 9, 102, 38, 416, 89, 71, 216,
728, 965, 818, 2, 38, 121, 195, 14, 326, 148, 234, 18, 55, 131, 234, 361, 824, 5,
81, 623, 48, 961, 19, 26, 33, 10, 1101, 365, 92, 88, 181, 275, 346, 201, 206, 86,
36, 219, 324, 829, 840, 64, 326, 19, 48, 122, 85, 216, 284, 919, 861, 326, 985,
233, 64, 68, 232, 431, 960, 50, 29, 81, 216, 321, 603, 14, 612, 81, 360, 36, 51, 62,
194, 78, 60, 200, 314, 676, 112, 4, 28, 18, 61, 136, 247, 819, 921, 1060, 464, 895,
10, 6, 66, 119, 38, 41, 49, 602, 423, 962, 302, 294, 875, 78, 14, 23, 111, 109, 62,
31, 501, 823, 216, 280, 34, 24, 150, 1000, 162, 286, 19, 21, 17, 340, 19, 242, 31,
86, 234, 140, 607, 115, 33, 191, 67, 104, 86, 52, 88, 16, 80, 121, 67, 95, 122, 216,
548, 96, 11 , 201, 77, 364, 218, 65, 667, 890, 236, 154, 211, 10, 98, 34, 119, 56,
216, 119, 71, 218, 1164, 1496, 1817, 51, 39, 210, 36, 3, 19, 540, 232, 22, 141, 617,
84, 290, 80, 46, 207, 411, 150, 29, 38, 46, 172, 85, 194, 39, 261, 543, 897, 624, 18,
212, 416, 127, 931, 19, 4, 63, 96, 12, 101, 418, 16, 140, 230, 460, 538, 19, 27, 88,
612, 1431, 90, 716, 275, 74, 83, 11, 426, 89, 72, 84, 1300, 1706, 814, 221, 132,
40, 102, 34, 868, 975, 1101, 84, 16, 79, 23, 16, 81, 122, 324, 403, 912, 227, 936,
447, 55, 86, 34, 43, 212, 107, 96, 314, 264, 1065, 323, 428, 601, 203, 124, 95, 216,
814, 2906, 654, 820, 2, 301, 112, 176, 213, 71, 87, 96, 202, 35, 10, 2, 41, 17, 84,
221, 736, 820, 214, 11, 60, 760.

图 21:比尔密码的第一页。

115, 73, 24, 807, 37, 52, 49, 17, 31, 62, 647, 22, 7, 15, 140, 47, 29, 107, 79, 84, 56,
239, 10, 26, 811, 5, 196, 308, 85, 52, 160, 136, 59, 211, 36, 9, 46, 316, 554, 122,
106, 95, 53, 58, 2, 42, 7, 35, 122, 53, 31, 82, 77, 250, 196, 56, 96, 118, 71, 140,
287, 28, 353, 37, 1005, 65, 147, 807, 24, 3, 8, 12, 47, 43, 59, 807, 45, 316, 101, 41,
78, 154, 1005, 122, 138, 191, 16, 77, 49, 102, 57, 72, 34, 73, 85, 35, 371, 59, 196,
81, 92, 191, 106, 273, 60, 394, 620, 270, 220, 106, 388, 287, 63, 3, 6, 191, 122, 43,
234, 400, 106, 290, 314, 47, 48, 81, 96, 26, 115, 92, 158, 191, 110, 77, 85, 197, 46,
10, 113, 140, 353, 48, 120, 106, 2, 607, 61, 420, 811, 29, 125, 14, 20, 37, 105, 28,
248, 16, 159, 7, 35, 19, 301, 125, 110, 486, 287, 98, 117, 511, 62, 51, 220, 37, 113,
140, 807, 138, 540, 8, 44, 287, 388, 117, 18, 79, 344, 34, 20, 59, 511, 548, 107,
603, 220, 7, 66, 154, 41, 20, 50, 6, 575, 122, 154, 248, 110, 61, 52, 33, 30, 5, 38, 8,
14, 84, 57, 540, 217, 115, 71, 29, 84, 63, 43, 131, 29, 138, 47, 73, 239, 540, 52, 53,
79, 118, 51, 44, 63, 196, 12, 239, 112, 3, 49, 79, 353, 105, 56, 371, 557, 211, 515,
125, 360, 133, 143, 101, 15, 284, 540, 252, 14, 205, 140, 344, 26, 811, 138, 115,
48, 73, 34, 205, 316, 607, 63, 220, 7, 52, 150, 44, 52, 16, 40, 37, 158, 807, 37, 121,
12, 95, 10, 15, 35, 12, 131, 62, 115, 102, 807, 49, 53, 135, 138, 30, 31, 62, 67, 41,
85, 63, 10, 106, 807, 138, 8, 113, 20, 32, 33, 37, 353, 287, 140, 47, 85, 50, 37, 49,
47, 64, 6, 7, 71, 33, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 191, 246, 85, 94, 511, 2,
270, 20, 39, 7, 33, 44, 22, 40, 7, 10, 3, 811, 106, 44, 486, 230, 353, 211, 200, 31,
10, 38, 140, 297, 61, 603, 320, 302, 666, 287, 2, 44, 33, 32, 511, 548, 10, 6, 250,
557, 246, 53, 37, 52, 83, 47, 320, 38, 33, 807, 7, 44, 30, 31, 250, 10, 15, 35, 106,
160, 113, 31, 102, 406, 230, 540, 320, 29, 66, 33, 101, 807, 138, 301, 316, 353,
320, 220, 37, 52, 28, 540, 320, 33, 8, 48, 107, 50, 811, 7, 2, 113, 73, 16, 125, 11,
110, 67, 102, 807, 33, 59, 81, 158, 38, 43, 581, 138, 19, 85, 400, 38, 43, 77, 14, 27,
8, 47, 138, 63, 140, 44, 35, 22, 177, 106, 250, 314, 217, 2, 10, 7, 1005, 4, 20, 25,
44, 48, 7, 26, 46, 110, 230, 807, 191, 34, 112, 147, 44, 110, 121, 125, 96, 41, 51,
50, 140, 56, 47, 152, 540, 63, 807, 28, 42, 250, 138, 582, 98, 643, 32, 107, 140,
112, 26, 85, 138, 540, 53, 20, 125, 371, 38, 36, 10, 52, 118, 136, 102, 420, 150,
112, 71, 14, 20, 7, 24, 18, 12, 807, 37, 67, 110, 62, 33, 21, 95, 220, 511, 102, 811,
30, 83, 84, 305, 620, 15, 2, 108, 220, 106, 353, 105, 106, 60, 275, 72, 8, 50, 205,
185, 112, 125, 540, 65, 106, 807, 188, 96, 110, 16, 73, 33, 807, 150, 409, 400, 50,
154, 285, 96, 106, 316, 270, 205, 101, 811, 400, 8, 44, 37, 52, 40, 241, 34, 205,
38, 16, 46, 47, 85, 24, 44, 15, 64, 73, 138, 807, 85, 78, 110, 33, 420, 505, 53, 37,
38, 22, 31, 10, 110, 106, 101, 140, 15, 38, 3, 5, 44, 7, 98, 287, 135, 150, 96, 33, 84,
125, 807, 191, 96, 511, 118, 440, 370, 643, 466, 106, 41, 107, 603, 220, 275, 30,
150, 105, 49, 53, 287, 250, 208, 134, 7, 53, 12, 47, 85, 63, 138, 110, 21, 112, 140,
485, 486, 505, 14, 73, 84, 575, 1005, 150, 200, 16, 42, 5, 4, 25, 42, 8, 16, 811,
125, 160, 32, 205, 603, 807, 81, 96, 405, 41, 600, 136, 14, 20, 28, 26, 353, 302,
246, 8, 131, 160, 140, 84, 440, 42, 16, 811, 40, 67, 101, 102, 194, 138, 205, 51,
63, 241, 540, 122, 8, 10, 63, 140, 47, 48, 140, 288.

图 22:比尔密码的第二页。

317, 8, 92, 73, 112, 89, 67, 318, 28, 96, 107, 41, 631, 78, 146, 397, 118, 98, 114,
246, 348, 116, 74, 88, 12, 65, 32, 14, 81, 19, 76, 121, 216, 85, 33, 66, 15, 108, 68,
77, 43, 24, 122, 96, 117, 36, 211, 301, 15, 44, 11, 46, 89, 18, 136, 68, 317, 28, 90,
82, 304, 71, 43, 221, 198, 176, 310, 319, 81, 99, 264, 380, 56, 37, 319, 2, 44, 53,
28, 44, 75, 98, 102, 37, 85, 107, 117, 64, 88, 136, 48, 154, 99, 175, 89, 315, 326,
78, 96, 214, 218, 311, 43, 89, 51, 90, 75, 128, 96, 33, 28, 103, 84, 65, 26, 41, 246,
84, 270, 98, 116, 32, 59, 74, 66, 69, 240, 15, 8, 121, 20, 77, 89, 31, 11, 106, 81,
191, 224, 328, 18, 75, 52, 82, 117, 201, 39, 23, 217, 27, 21, 84, 35, 54, 109, 128,
49, 77, 88, 1, 81, 217, 64, 55, 83, 116, 251, 269, 311, 96, 54, 32, 120, 18, 132, 102,
219, 211, 84, 150, 219, 275, 312, 64, 10, 106, 87, 75, 47, 21, 29, 37, 81, 44, 18,
126, 115, 132, 160, 181, 203, 76, 81, 299, 314, 337, 351, 96, 11, 28, 97, 318, 238,
106, 24, 93, 3, 19, 17, 26, 60, 73, 88, 14, 126, 138, 234, 286, 297, 321, 365, 264,
19, 22, 84, 56, 107, 98, 123, 111, 214, 136, 7, 33, 45, 40, 13, 28, 46, 42, 107, 196,
227, 344, 198, 203, 247, 116, 19, 8, 212, 230, 31, 6, 328, 65, 48, 52, 59, 41, 122,
33, 117, 11, 18, 25, 71, 36, 45, 83, 76, 89, 92, 31, 65, 70, 83, 96, 27, 33, 44, 50, 61,
24, 112, 136, 149, 176, 180, 194, 143, 171, 205, 296, 87, 12, 44, 51, 89, 98, 34, 41,
208, 173, 66, 9, 35, 16, 95, 8, 113, 175, 90, 56, 203, 19, 177, 183, 206, 157, 200,
218, 260, 291, 305, 618, 951, 320, 18, 124, 78, 65, 19, 32, 124, 48, 53, 57, 84, 96,
207, 244, 66, 82, 119, 71, 11, 86, 77, 213, 54, 82, 316, 245, 303, 86, 97, 106, 212,
18, 37, 15, 81, 89, 16, 7, 81, 39, 96, 14, 43, 216, 118, 29, 55, 109, 136, 172, 213,
64, 8, 227, 304, 611, 221, 364, 819, 375, 128, 296, 1, 18, 53, 76, 10, 15, 23, 19, 71,
84, 120, 134, 66, 73, 89, 96, 230, 48, 77, 26, 101, 127, 936, 218, 439, 178, 171, 61,
226, 313, 215, 102, 18, 167, 262, 114, 218, 66, 59, 48, 27, 19, 13, 82, 48, 162, 119,
34, 127, 139, 34, 128, 129, 74, 63, 120, 11, 54, 61, 73, 92, 180, 66, 75, 101, 124,
265, 89, 96, 126, 274, 896, 917, 434, 461, 235, 890, 312, 413, 328, 381, 96, 105,
217, 66, 118, 22, 77, 64, 42, 12, 7, 55, 24, 83, 67, 97, 109, 121, 135, 181, 203, 219,
228, 256, 21, 34, 77, 319, 374, 382, 675, 684, 717, 864, 203, 4, 18, 92, 16, 63, 82,
22, 46, 55, 69, 74, 112, 134, 186, 175, 119, 213, 416, 312, 343, 264, 119, 186, 218,
343, 417, 845, 951, 124, 209, 49, 617, 856, 924, 936, 72, 19, 28, 11, 35, 42, 40, 66,
85, 94, 112, 65, 82, 115, 119, 236, 244, 186, 172, 112, 85, 6, 56, 38, 44, 85, 72,
32, 47, 73, 96, 124, 217, 314, 319, 221, 644, 817, 821, 934, 922, 416, 975, 10, 22,
18, 46, 137, 181, 101, 39, 86, 103, 116, 138, 164, 212, 218, 296, 815, 380, 412,
460, 495, 675, 820, 952.

图 23:比尔密码的第三页。

1862年,84岁高龄的莫里斯知道,他正在走向生命的尽头,他将不得不与他人分享比尔密码的秘密。否则,任何实现比尔愿望的可能都将随他的死亡而烟消云散。莫里斯相信他的一个朋友可以完成,但不幸的是这个人的身份到现在都是一个谜。关于莫里斯的这个朋友,所有我们知道的就是他在1885年写了这本小册子,所以在以下部分我将简单地称他为"作家"。作家在那本小册子中解释了他匿名的原因:

> 我已预见这本书的广为流行,但为避免从全国各地发来的各种信件的干扰,无非是提出各种问题请我回答,这将占用我全部的时间而改变我这项任务的性质。我已决定从出版物上撤消我的名字,我对所有对此感兴趣的人保证,我已把我所有知道的东西全部奉献出来了,我也不可能在这里的陈述中再加一句额外的话。

为保护他的身份,作家请了当地社区令人尊敬的一位乡村道路测量员詹姆斯·B·瓦特先生作为他的代理和发行人。

所有我们所知的关于这个奇异的比尔密码的传说都写在了这本小册子上,因此还得感谢这位作者使我们拥有了这个密码和莫里斯讲的故事。不仅如此,作家还成功地破解了第二个比尔密码。和第一、第三个密码一样,第二个密码也是由一页数字组成。作家认为每个字母可能代表一个字母,但是数字的范围却远远超过字母表中字母的数目,因此作家想到他要破解的密码可能是用几个数字代表一个字母。而有一种密码具有这样的特性,那就是所谓"书卷密码",其中一本书或者一篇文章本身就是密钥。我们姑且称这样的书或文章为钥文。

首先,密码编码者顺序地给钥文的每个单词编号,这样每个数字就可用来代替关联单词的第一个字母,例如下面一段话:1For

2example, 3if 4the 5sender 6and 7receiver8agreed 9that 10this 11sentence 12were 13to 14be 15the 16keytext, 17then 18every 19word 20would 21be 22numerically 23labeled, 24each 25number 26providing 27the 28basis 29for 30encryption.(意思为:例如,如果发送者和接收者都知道这句话是钥文,那么每个单词将被标上数字,在这些数字的基础上加密。)

下面,我们作出一张表来标出每个数字及其关联单词的首字母:

1 = f	11 = s	21 = b
2 = e	12 = w	22 = n
3 = i	13 = t	23 = t
4 = t	14 = b	24 = e
5 = s	15 = T	25 = N
6 = a	16 = K	26 = P
7 = r	17 = T	27 = T
8 = a	18 = e	28 = b
9 = t	19 = w	29 = 4
10 = t	20 = w	30 = e

现在,可以根据上面这个表,通过将明文中的每个字母替换成数字来加密一个信息。明文中的 f 将被替换成 1,字母 e 被替换成 2,18,24 或 30。因为我们的钥文是个短句子,我们没有用来替换的,诸如 x 和 z 的数字,但我们却有足够的代替者来加密单词比尔,它可能是 14 - 2 - 8 - 23 - 18。如果接收者有一个该钥文的拷贝,那么解密信息将是小事一件。然而如果第三方只截获了密文,那么对其进行密码破译就要依赖于如何确定钥文这个问题上。作家写道:“带着这种想法,我对我所有能弄到的书做了一个测试,给

When, in the course of human events, it becomes [10]necessary for one people to dissolve the political bands which [20]have connected them with another, and to assume among the [30]powers of the earth, the separate and equal station to [40]which the laws of nature and of nature's God entitle [50]them, a decent respect to the opinions of mankind requires [60]that they should declare the causes which impel them to [70]the separation.

We hold these truths to be self-evident, [80]that all men are created equal, that they are endowed [90]by their Creator with certain inalienable rights, that among these [100]are life, liberty and the pursuit of happiness; That to [110]secure these rights, governments are instituted among men, deriving their [120]just powers from the consent of the governed; That whenever [130]any form of government becomes destructive of these ends, it [140]is the right of the people to alter or to [150]abolish it, and to institute a new government, laying its [160]foundation on such principles and organizing its powers in such [170]form, as to them shall seem most likely to effect [180]their safety and happiness. Prudence, indeed, will dictate that governments [190]long established should not be changed for light and transient [200]causes; and accordingly all experience hath shewn, that mankind are [210]more disposed to suffer, while evils are sufferable, than to [220]right themselves by abolishing the forms to which they are [230]accustomed.

But when a long train of abuses and usurpations, [240]pursuing invariably the same object evinces a design to reduce them [250]under absolute despotism, it is their right, it is their [260]duty, to throw off such government, and to provide new [270]Guards for their future security. Such has been the patient [280]sufferance of these Colonies; and such is now the necessity [290]which constrains them to alter their former systems of government. [300]The history of the present King of Great Britain is [310]a history of repeated injuries and usurpations, all having in [320]direct object the establishment of an absolute tyranny over these [330]States. To prove this, let facts be submitted to a [340]candid world.

图 24:《独立宣言》的开头三段,每 10 个单词标一次号,这是第二页比尔密码的密钥。

每个字母标号,再与比尔密文中的数字作比较。这样做几乎都是徒劳的,然而等到检验《独立宣言》这篇文章时,我发现它和比尔密码中的某一页有关联,这又燃起了我的希望。”

《独立宣言》原来就是第二页比尔密码的钥文,对宣言中的单词编号即可破译它们。图 24 显示了《独立宣言》的开头部分,我简单地把每 10 个单词标一次号以帮助读者明白是怎么破译这个密码的。图 22 是密文,第一个数字是 115,宣言中的 115 个单词是“instituted”,因此密文中第一个数字代表 i。密文第二个字母是 73,宣言中第 73 个单词是“hold”,因此第二个字母是 h。下面是取自小册中的整篇破译出的明文:

I have deposited in the country of Bedford, about four miles from Buford's, in an excavation or vault, six feet below the surface of the ground, the following articles, belonging jointly to the parties whose names are given in number “3” herewith: The first doposet consisted of one thousand and fourteen pounds of gold, and three thousand eight hundred and twelve pounds of silver, deposited November, 1819. the second was made December, 1821, and consisted of nineteen hundred and seven pounds of gold, and twelve hundred and eighty - eight pounds of silver; alse juwels, obtained in st, Louis in wxchange for silver to save transportation, and valued at $ 13,000. The above is swecurely packed in iron pot, with iron covers. The vaults is roughly lined with stone, and the cessels rest on solid stone, and are covered with others. Paper numver “1” describes the exact locality of the vault, so that no difficulty will be had in finding it.(大意为:我已把财宝埋藏在距布福德家约 4 英里的贝德福德镇上的一个六尺深的洞穴中,下面的东西是共同属于我和我的同伴的,他们的名字写在第 3 页纸上。

第一批埋藏物包括 1014 磅重的黄金,3820 磅白银,于 1819

年 11 月存放。第二批存于 1821 年 11 月，包括 970 磅黄金，1288 磅白银以及价值 13000 美元的珠宝，珠宝是在圣路易斯为了节省运费用白银换来的。

以上被安全地放在一些带铁盖的铁罐里，洞穴里塞有一些石头，容器就摞起搁在石头上。第一页纸上描述了洞穴的确切地点，因此找到它不会很难。)

值得注意的是密文中含有一些错误。例如解密时单词"four miles(4 英里)"中的 u 是根据宣言中的第 95 个单词来的，然而第 95 个单词是"inalienable(不能剥夺的)"。因此这也许是因为比尔的粗心，也可能是比尔使用的宣言中第 95 个单词是"unalienable"，在《宣言》19 世纪的版本中，确实有过这个单词。不管怎样，这次成功的破译，明白地显示了这批财宝的价值——以今天的金银价格，至少 2000 万美元。作家知道了这批珠宝的价值之后，便花了无数的时间来分析其他两页密码，特别是第一页比尔密码，其中描述了珠宝的埋藏地点。这也在情理之中，然而这个密码除了使他精力耗尽，就只剩下悲哀了：

> 由于花了大量的时间来研究它，我已经从相当富有沦落到绝对贫穷的地步。我的义务本来是保护它，而我的眼睛却像蒙了布一样违背了他们的意愿。最终我看清了他们的愿望，我决定立刻并永远地断绝所有与此事的联系，尽可能地弥补我的错误。为此，我觉得能够使诱惑远离我最好的方法是把整个事情公开，我也就将我肩上的责任又转给了莫里斯先生。

这样，该密码以及作家知道的一切于 1885 年就出版了。虽然一次仓库大火烧毁了大部分的小册子，但是存留的那些还是在林奇伯格引起了不小的震动。被比尔密码吸引的诸多觅宝者当中，

最热情的要属哈特兄弟：乔治和克莱顿。几年来他们一直凝思剩余的两页密码，进行了各种各样的密码破译试验，有时他们甚至以为已经找到了答案。对于一个没有非分之心的人来说，破译这个密码纯粹是一种思维的享受；而对于另有所图的觅宝者们，这完全就是另外一回事了。哈特兄弟的一种寻宝方法就是用炸药炸开一个特定的范围，很遗憾，炸开的坑里没有任何黄金的踪迹。克莱顿于 1912 年就放弃了，而乔治继续钻研比尔密码直到 1952 年。另一个更固执的比尔密码迷是海勒姆·赫伯特，他 1923 年迷上比尔密码，一直持续到 70 年代才罢手。他也一样没有任何收获。

专业密码破译师也开始追寻比尔财宝的踪迹。赫伯特·O·亚德利，他在一战末建立了美国密码局(即美国的密室)，也对比尔密码产生了兴趣。同样，20 世纪前半世纪美国密码分析学界的领导人物科洛奈尔·威廉姆也迷上了比尔密码。当威廉姆负责情报服务研究时，他将比尔密码作为训练计划的一部分。据他妻子所说，他认为该密码具有相当的灵活性，特别设计用来迷惑那些轻信的读者。他 1969 年死后建立的弗里德曼文档经常被军方历史学家参考，但是更多的是热心的比尔迷，他们希望能得到这位专家的指点。再近些时候，寻觅比尔宝藏大军中的一位主要人物是卡尔·哈默，他是计算机公司的一位退休主管，也是计算机密码学的先驱之一。据哈默所说："比尔密码已经占据了这个国家中至少 10% 的最优秀的密码破译家的思想，他们都不遗余力，这项工作即使最终走进了一个死胡同也大大促进并改善了计算机研究。"哈默也是"比尔密码和财宝协会"中著名的一员。该协会成立于 20 世纪 60 年代，旨在激起人们对比尔传奇的兴趣。开始协会要求任何发现宝藏的成员要与其他成员共享，但是这项规定似乎阻止了许多比尔密码探索者的加盟，因此协会很快就取消了这个要求。

尽管协会中业余觅宝者和专业密码破译师的联合努力，第一和第三页比尔密码一个世纪来一直是个谜。黄金、白银和珠宝始

终没有发现。解密时许多尝试都围绕着第二页比尔密码的钥文——《独立宣言》。当然直接地给宣言的单词编号对第一和第三页密码没有任何作用,密码破译师尝试了其他的方法,例如给单词从后向前编号或者间隔着来编号。但到目前为止,没有一个奏效的。关于第一页密码中有一个问题是它含有的数字高达 2906,而《独立宣言》中只有 1322 个单词。因此其他的文章和书籍也被考虑作为钥文,也有许多密码分析师已经在研究一个完全不同的加密系统的可能性。

你或许对这个没有破解的比尔密码的持久性感到惊奇,尤其是我们记得在写密码者和破密码者之间的战争中,一般都是破密码者占上风。巴比奇和卡西斯基发明了破解维热纳尔密码的方法后,密码编码者一直努力寻找能够代替它的密码。而比尔是怎么提出这么一个坚不可摧的东西呢?原因是从比尔密码创造的那一刻起,密码编码者就拥有了一个绝对的优势。信息是一次性的,因为它们关系到如此贵重的一个宝藏,比尔或许准备为第一和第三页密码写一篇特别的一次性钥文。事实上,如果钥文真的由比尔亲笔所写,这也就解释了为什么搜寻已出版的文章而没有结果的原因。我们可以试想比尔写了一篇 2000 字的私人文章,可能就是关于捕猎野牛的事情,而这篇文章只有一份。只有这篇文章的持有者,即拥有了独一无二的钥文,才能够破译第一页和第三页比尔密文。比尔曾提到他把钥文留给了一位在圣路易斯的朋友,但是如果这个朋友丢了或毁坏了钥文,那么密码破译者们将永远不能破解比尔密码。

为一个信息专门写一篇一次性的钥文要比使用一本出版的书作为钥文安全得多。但这需要发送者有时间写出钥文并能够传给接收者,而这个要求对于每日通讯来说是不可能的。

在比尔的例子中,他可以在空闲的时候写好钥文,然后在路过圣路易斯的任何时候把它交给他的朋友,最后一旦需要挖掘宝藏,

就将它邮寄出去。

一种解释比尔密码无法破译的说法是小册子的作者在出版之前，对密码进行了有意的窜改。或许作者仅仅是想套出在圣路易斯比尔朋友手中的钥文。如果他确切无误地发表了密码，那么那个朋友就可能破译它然后取出黄金，这个作者也将一无所获。然而如果这个密码被改动过，那么那位朋友会最终认识到他需要这位作者的帮助，就会联系出版商瓦德，瓦德会相应地联系作者。这位作者然后再拿出正确的密码作为交换，取得财宝的一份。

也有可能是这批财宝在几年前就已被发现，而发现者偷偷地背着当地居民将财宝运走了。比尔迷特别倾向于一种说法，即国家安全局(NSA)已经发现了这个宝藏。美国政府密码机构拥有世界上最强大的计算机和最具才华的头脑，他们可能已经发现关于密码的一些秘密却没有公开。美国国家安全局很少公开过什么事情，有人提议 NSA 不是用来指 National Security Agency(国家安全局)，而是指“Never Say Anything(沉默主义者)”或“No Such Agency(没有这样的机构)”。

最后我们也不能排除一种可能性，那就是比尔密码从头到尾是个有意的愚弄，比尔这个人根本不存在。怀疑论者认为这个匿名的作者受埃德加·阿兰·波的《金甲虫》启发，虚构了整个故事，并印成小册子，利用一些人的贪欲来获利。愚弄观点的支持者搜寻了比尔故事中的矛盾和错误之处。例如根据小册子所说，比尔的信被锁在铁盒里并写于 1822 年，其中含有一个单词“stampede(惊跑)”，而这个单词直到 1834 年才出现在印刷物上。但也很有可能这个单词在美国西部更早地被使用，比尔在他的旅途中学到了这个词。

怀疑论者中有一位是最坚定的，他是位密码编码师叫路易斯·克鲁。他声称已经发现证明比尔的信是由小册子的作者所写，就是那封据说从圣路易斯发出的信和铁盒里的信。他对作者的文字

和比尔的文字做了一次分析，看看其中有无相似性。克鲁比较了几个方面，诸如句子开头使用“The”、“Of”和“And”的频率；每句中逗号和分号的平均数目以及写作风格——否定词、不定冠词、关系从句和被动句型的使用等。

除了比较作者和比尔的文字，克鲁还分析了19世纪其他三个弗吉尼亚州人的文字。在这五套文字中，只有比尔和小册子作者的文字具有高度的相似性，这表明它们可能为同一个人所写。换句话说，这意味着作者可能捏造了比尔的信并虚构了整个故事。

另一方面，也有各方面的证据表明比尔密码的真实性。首先，如果没有破译的比尔密码是个骗局，我们可以认为制造这个骗局的人应该是随意地选择一些字母。然而这些数字却有着各种复杂的模式。例如我们用《独立宣言》做为密钥给第一页密码解密时，虽然没有产生有意义的单词，但它确实给出了诸如 abfdefghi-ijklmmnohpp 这样的序列。虽然它不是完全按照字母表的顺序，但它显然不是随机的。美国密码协会的詹姆斯·吉尔格利不相信比尔密码是真实的，但他计算了这样一个随机序列出现的概率大约是一千万分之一，表明在第一页的密码中有某种潜在的密码编码原则在里面。一种理论认为《独立宣言》确实就是密钥，但是根据它解密后的文章需要第二次的解密，也就是第一页比尔密码被加密了两次，即所谓超加密。上面出现的字母表顺序的序列可能就是一种好的现象，暗示第一步解密工作已成功地完成。

支持密码存在的进一步证据来自历史学家的研究，他们似乎证实了托马斯·比尔的故事。彼特·维迈斯特是当地的一个历史学家，他在他的《比尔宝藏——神秘的历史》一书中收集了许多研究证据。维迈斯特首先提出疑问有没有证据表明托马斯·比尔这个人是存在的。维迈斯特查阅了1790年的人口普查资料和其他一些文件发现了在弗吉尼亚有几个叫托马斯·比尔的人，但他们的背景与已知的细节不太吻合。维迈斯特研究了小册子中的其他细

节，例如比尔曾去过圣达菲并且发现了金子。终于发现 1820 年美国夏安族曾有一个传说，大意是在西部曾发现过金银，后来被埋到东部的山里。而且 1820 年圣路易斯的邮政记录里有托马斯· 比尔的人名，这符合小册子所说的比尔在 1820 年离开林奇伯格后曾西行经过圣路易斯。小册子也提到 1822 年比尔曾从圣路易斯发过一封信。

所以对比尔密码的传说似乎确实有些依据，结果它继续吸引着密码破译师和觅宝者，其中包括约瑟夫·雅西克、玛里琳·帕森以及他们的一只狗——缪夫茵。1983 年 2 月的一天夜里，他们在观山教堂墓地挖宝时被抓获，后被指控侵犯死者墓地。他们除了发现棺材没有任何收获，还不得不在监狱度过周末并罚款 500 元。这些业余的掘墓者或许在听了关于梅尔·费希尔的故事之后会稍稍感到安慰。梅尔·费希尔是个专业的探宝者，1985 年他发现了在佛罗里达州基韦斯特沉没的一艘西班牙大帆船，从中打捞了价值近 4 千万美金的黄金。但是比尔带给他的遭遇却并不比上面的掘墓者好到哪儿去。1989 年 9 月，佛罗里达的一位比尔专家告诉了他一个秘密，他认为比尔的财宝应埋藏在弗吉尼亚州贝德福德市的格雷厄姆工厂的下面。于是费希尔聚集了一组投资者，为避免外界怀疑，以沃达的名义买下了这块地皮。虽然他挖了好久，但是却一无所获。

一些探宝者放弃了破解这两页密码的希望，将注意力转向已经破译的那一页密码上。例如第二页密码除了说明宝藏的内容，还提到了它埋藏距布福德 4 英里的地方。这可能是指布福德村或者更具体一点布福德酒馆，标在图 25 的中央。密码也提到“洞里填满了石头”。因此许多探宝者沿着古斯克瑞克城搜寻，那里有大量的石头。每年夏天这个区域都吸引着满怀希望的人，一些人装备着金属探测器，还有人带着物理学者和占卜者。布福德周围的城镇有许多商人，他们乐滋滋地向外出租各种装备，包括工地挖掘

机。当地的农场主显然不欢迎这些陌生人,因为他们经常践踏他们的田地,毁坏他们的篱笆并挖出许多巨大的洞穴。



图 25:1891 年美国地质测量图的一部分,显示了在第二页密码上指明的布福德及其周围 4 英里的范围的地形。

读完比尔密码传奇之后,你或许已经跃跃欲试想挑战一下自己吧!这个至今未破解的 19 世纪的密码,以及价值 2000 万美元的财宝所产生的诱惑可能是无法抵挡的。但是在你准备这次宝藏之旅之前,请先读一读小册子的作者给你的忠告。

在将这些资料公开之前，我想对那些有兴趣的人先说一句话，以我自己痛苦的经历给他们一点建议。那就是：保证正常的工作，利用空余时间来研究它，如果你没有任何空闲时间那就不要理会这件事……千万不要再像我那样，牺牲你和你家人的利益来做一些可能无法做到的事情；正如我已说过的，当你一天的工作完成后，你可以舒适地坐在暖炉旁尽情研究，短时间的投入不会损害任何人，或许还会有所回报。

第三章 加密的机械化

在19世纪末,密码编码学处于一种混乱状态。自从巴比奇和卡西斯基破坏了维热纳尔密码的安全性之后,密码编码师一直在寻找一种新的密码,希望能够重新建立秘密通讯,这样商人和军人可以充分利用电报的快捷而不必担心他们的通讯被窃取和解密。而且,在20世纪初,意大利物理学家马可尼发明了一种更为强大的电信手段,这使得安全加密的需要更为紧迫。

1894年,马可尼开始做实验研究电线的一种奇怪的特性。在特定条件下,如果一根电线带有电流将会诱使一定距离以外的另一根线路中产生电流。马克尼改进了两个线圈的设计,提高了电流强度并增加了天线,很快他能够跨越达2.5公里来传送和接收信息。

他发明了无线电。当时有线电报已经出现了将近半个世纪了,但这需要在发送者和接收者之间建立一条线路来传送一个信息。马可尼系统具有很大的优势就是无线传送——空中信号。1896年为了寻找经济支持,马可尼移民到英国,在那里他申请了第一个专利。他继续做他的实验并不断增加了无线通讯的距离,先是跨越了长达15公里的布里斯托尔海峡,然后又成功地跨越53公里的英吉利海峡将信号传到了法国。与此同时,他开始为他

的发明寻求商业应用，他向一些支持者提出了无线通讯的两大优点：第一，它不需要建立昂贵的通信线路；第二，它可以跨地区地传送信息。1899 年他专门向公众做了一次精彩的演示，当时世界最主要的快艇赛：美国杯快艇赛，正在进行，他在两艘船上装备了无线电，使记者能够及时地将报道传到了纽约，第二天的报纸就刊登了美国杯新闻。

当时评论家指出由于无线电波不能够弯曲，所以不能沿着地球表面前进，因而无线电传送也只能在 100 公里左右。马可尼则进一步作实验推翻了这种无线电受地平线限制的说法，他在康沃尔发出一条信息，试图在纽芬兰接受此信号，距离大约有 3500 公里。1901 年 12 月，每天有 3 小时，康沃尔的传送员一次次地发送字母 S(莫尔斯电码表示为三个点)，而马可尼则站在纽芬兰的悬崖上，顶着寒风试图探测无线电信号。就这样日复一日却没有结果。一天马可尼艰难地放起一个巨大的风筝，上面带着天线。在 12 月 12 日午时过后，马可尼终于接收到了三个微弱的点信号，这也是第一个跨越大西洋的信息。其实对于马可尼的成功直到 1924 年才有解释，当时物理学家发现距地面约 60 公里的大气层为电离层。电离层就像一面镜子，使无线电波在上面发生了反射。无线电波也可以在地球表面发生反射，因此事实上无线电经过一系列地表和电离层的反射之后可以到达地球的任何地方。马可尼的成功使人们对无线电的兴趣更加浓厚。

马可尼的发明使得军方极为苦恼，无线电带给他们的既是激动又是惧怕。无线电的技术优势是明显的：它使地区任意两点间的无线通讯成为可能，如果建设这样一条线路，那是不切实际的，甚至不可能。有一段时间，一个身在港口的海军长官由于没有任何方法联系他的船队，导致他的船队失踪了几个月，现在有了无线电，无论船队在什么地方，这位长官都能够指挥它们。同样，无线电会使将军在战争中时刻与军队保持联系，从而指挥战斗。无线

电使所有的这一切成为可能，它沿着各个方向发送信息，无论接收员在何地都能收到信息。但是无线电这种强大的渗透性也是军事上存在的最大弱点，因为就像信息到达接收者手中一样，它也会不可避免地到达敌人手中。因此最终可靠的加密系统就变得非常必要。敌人能够截住每一个信息，而密码编码师则寻求各种方法来阻止敌人破译这些信息。

因此无线电具有双重特性——易通信性和易拦截性，这在一战爆发后表现得尤为突出。所有成员都想充分发掘无线电的资源，却苦于不知如何保障安全。无线电在经历了一战之后，有效的加密系统成了急需解决的问题。大家都希望能有一个突破，创立一些新的密码来保护军事秘密。然而从 1914 到 1918 年，没有什么大的发现，仅多了些失败的例子。密码编码者提出了几个新密码，但一个个均被破解了。

其中战争时期著名的一种密码是德军 ADFGVX 密码。1918 年 3 月 5 日被最初使用，不久后即 3 月 21 日德军就开始了一次主攻。像以往任何一次进攻一样，这次主攻同样要求出奇制胜。由密码编码师组成的一个小组从各种密码中选择了 ADFGVX 密码，他们认为这个密码是最隐秘的。事实上他们相信它是不可破解的。这个密码的特点在于它错综复杂，综合了替换和移位两种处理方法。

1918 年 6 月初，德军炮兵距巴黎仅有 100 公里，正为最后一次推进作准备。盟军惟一的希望就是破解 ADFGVX 密码以知道德军在他们的防守前究竟选择那一点开始突破。幸运的是，他们还有一个"密码武器"，密码破译学家乔治斯·佩因芬先生。这个又黑又瘦的法国人拥有一个洞察力极强的头脑，一战爆发后，他曾与密码机构的一位成员会了一次面，也就是这一次他在解决密码难题上的才能被发掘了出来。从此以后，他这种难得的才能就专门用于发现德军密码的弱点。为了破解 ADFGVX 密码，他经受了

无数个不眠夜，体重下降了 15 公斤。

最终在 6 月 2 日的晚上，他破解了一段 ADFGVX 信息。佩因芬的突破导致了一系列其他密码依次被破解，其中有条信息含有一个命令“急需军需品”，该信息表明它是从大约巴黎以北 80 公里的某个地方发出来。德军如此紧急地需要军需品表明这个地方必定是德军即将展开进攻的地点。随后的空中侦察证实了这一点。盟军士兵随即被送到前线地带支援，一个星期后，德军攻势展开了。由于不再是他们想像中的趁人不备，德军在经历了持续五天恶梦般的战斗之后大败而归。

ADFGVX 密码的破解成了一战期间密码学的典型。尽管产生了无数的新密码，但它们无非是 19 世纪已经破解了的密码的变形或组合。尽管其中有些密码开始时确实提供了某种程度的安全保障，但它们毫无例外的都是“短命”，因此密码破译师很快就征服了它们。对于密码破译师来说，最大的问题是如何应付信息数量的急剧增长。在无线电出现之前，能够被截获的信息很少并且很珍贵，密码破译师对每一个都非常珍惜。然而到了一战期间，无线电的使用激增，而每个信息都能够被截获，一批批的密文摆在密码破译师的面前等待他们去破译。据估计法国在第一次世界大战期间共截获的德国通讯信息达 1000 万个单词。

在战争期间，所有的密码破译师中法国人的效率最高。在战前，他们已经拥有当时欧洲最强大的密码破解队伍，这也是有历史缘由的。1870 年，拿破仑三世为了急于恢复他的声望，对普鲁士发动了进攻。但是他没有料到处于北方的普鲁士会和南方的德国形成联盟。在俾斯麦的领导下，普鲁士军队重挫了法军，并吞并了阿尔萨斯和洛林省，从而结束了法国在欧洲的统治时期。法国人受到羞辱，而同时新联合的德国给法国造成更大威胁，这种形势下法国密码破译师受到了激励，觉得有必须掌握必要的技能以提供详细的情报来监视敌国的行动。

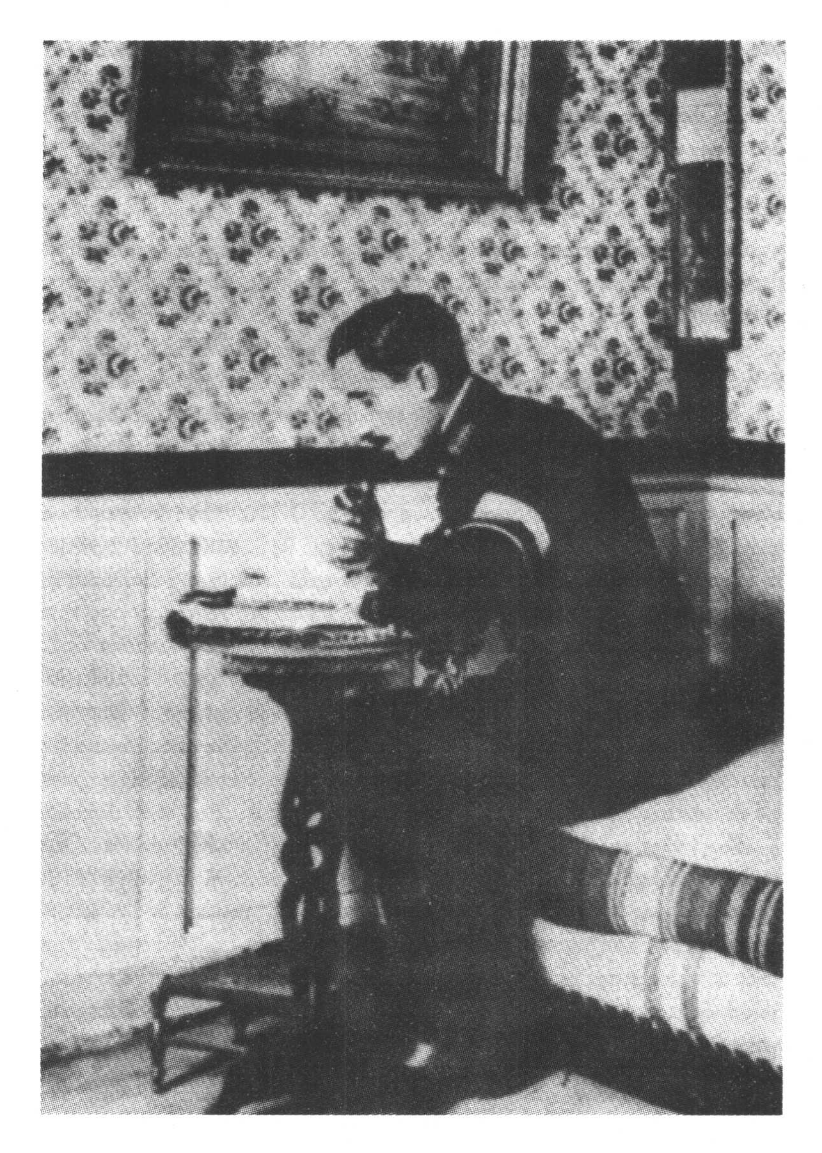


图 26:乔治斯·佩因芬中尉

正是在这种情况下,奥古斯特·克科霍夫斯写出了《密码学》。

尽管克科霍夫斯是个荷兰人,但他大部分时间是在法国,他的著作为法国人提供了关于密码分析学原理的一个优秀的指导。三十年后一战开始的时候,法军已经充分完善了克科霍夫斯的思想。正当像佩因芬这样孤独的天才在寻求破解新的密码的时候,在法国已有成组的密码破译部门,每组都具有破解特定密码的熟练技能,开始日复一日地投身于密码破译当中。战争的时候,时间就是一切,密码破译师就像传送带一样,快速有效地提供情报。

公元前400年,中国的孙子在他的著作《孙子兵法》中提到:"三军之事,莫亲于间,赏莫厚于间,事莫密于间。"(大意为:在军队中,没有比间谍更为亲近的人,给予奖赏时,没有比间谍更为优厚的,没有什么事情比间谍更为秘密。)法国人坚信孙子的话,他们在磨练破译密码技能的同时,还发展了几个收集无线电情报的辅助技术。这些辅助技术与密码破译并无关系,例如,法国监听员学会了如何辨别一个无线电操作员的"手迹",一旦一条加密的信息以莫尔斯电码的形式发送出来,它就变成了一系列的点和短横,而我们可以通过分析每个无线电操作员的传送速度,他的停顿以及点和短横的相对长度来确定他们的身份。事实上,上述这些特征就相当于一个人的笔迹,而笔迹是可以辨认的。此外,法国人还建立了六个方向搜索站,它们能够检测每个信息发自哪里。每个站点不断移动它的天线直到收到的信号最强烈,这就确定了信息源的一个方向。通过组合两个或两个以上站点的信息方向,就可能定位出敌方传送线的确切源头。再加上第一条信息即操作员的手迹,就可能确立某特定军营的身份和地点。法国的情报员可以在几天内跟踪它的走向,一般能推出某敌军部队的目的地和军事目的。这种形式的情报搜集被称作信道分析,它在一个新的密码出现后,前期显得非常有用。对于每个新密码来说,密码分析师可能暂时无法破解它,但即使一个信息无法破译,信道分析仍会提供一些有用的信息。

德军的态度和法国的警觉形成了鲜明的对比,它甚至没有任何的军方密码破译机构就进入了战争。直到1916年,德军才建立了一个专门截获盟军信息的组织。这么迟建立这个组织的部分原因是这样的:德军在战争前期就挺进到了法国领土,法国在撤退过程中摧毁了陆上通讯电缆线路,迫使德军不得不依赖无线电通讯。然而这使得法国能够连续不断地截获德军通讯,当法军撤退到安全地带时,他们拥有自己的陆上通讯电缆线路因而没有必要通过无线电来通讯。而对于德国来说,由于法国的无线通信很少,他们很难有所截获,所以他们就战争前两年内没有急于发展他们的密码破译部门。

英国和美国对盟军的密码破译也做出了重要的贡献。有个例子很好地说明了盟军密码破解者的优势地位以及他们对一战的影响。这是关于1917年1月17日,英国截获了一个德军电报,破解这个电报的故事说明了密码破译师是如何最大程度地影响战争的局势,也说明了使用不合格的加密系统所带来的灾难性后果。也就是几个星期后,这个被解密的电报迫使美国的重新思考了它的中立政策,并直接改变了战争的平衡点。

尽管来自英国和美国政治家的呼声不断,威尔逊总统在战争的前两年内,始终坚定地拒绝派遣美军部队支援盟军。除了不想在欧洲的战场上牺牲自己国家的年轻生命以外,他还坚信这场战争只能通过和平谈判来解决,他相信如果他保持中立,做一个调解者,他能够最好的为这个世界作出贡献。1916年,德国指定了一位新的外交大臣阿瑟·齐默尔曼,威尔逊看到了和平解决的希望。这个身材魁梧又面善和气的外交大臣,似乎预示了德国开明政策时代的到来,美国的新闻报纸头版刊出了"我们的朋友齐默尔曼和德国的开明化",一篇文章把他称为"德美关系未来的最好的预兆"。然而,美国人不知道,齐默尔曼没有任何寻求和平的打算。相反他正在计划扩大德军的进攻范围。

回到1915年，一艘德国潜艇炸沉了一艘远洋客轮“路西塔尼亚号”，1198名乘客被溺死，包括128名美国公民。此后德军再三保证，为了避免偶然伤及平民船只事件的再度发生，从此以后德军潜艇攻击前将浮出水面，如果德军不这样道歉，“路西塔尼亚号”的沉没将使美国卷入战争。然而，1917年1月9日齐默尔曼参加了在德国普莱斯城堡的一个重要会议，在那儿最高司令部正尽力说服德国皇帝是打破他们诺言的时候了，他们旨在开展一场没有限制的水下战争。德军司令官知道如果他们的潜艇保持在水下发射鱼雷的话，那将是战无不胜的。他们相信这将是决定战争结果的一个关键性因素。最高司令部指出无限制的潜艇攻击将切断英国的供应航线，从而能在六个月内迫使他们投降。

速战速决是精要所在，德军当然知道无限制的水下战争必然导致更多无辜的美国平民船只的沉没，也几乎必然地迫使美国对德军宣战。这样的话，德军需要在美军部队行动之前先占领一个国家，在欧洲战场上制造一些影响。在普莱斯召开的会议末期，德国皇帝最终相信了速战速决是可行的，他签署了一个命令，发动无限制潜艇战争，并于2月1日有效。在剩下三个星期内，齐默尔曼实行一个防护性政策。如果无限制水下战争增加了美军参战的可能性，那么齐默尔曼就有一个计划将延缓美军进入欧洲战场，甚至有可能完全使美国失去参战的勇气。齐默尔曼的想法是和墨西哥联盟，说服墨西哥总统进攻美国，收回诸如得克萨斯、新墨西哥以及亚历桑那的领土。德军将在经济和军事上支持墨西哥对付共同的敌人。

不仅如此，齐默尔曼还希望墨西哥总统，能够扮演一个中间人的角色去说服日本也进攻美国。这样的话，德军对美国的东海岸造成威胁，日本从西面进攻，而墨西哥从南面侵入。齐默尔曼主要的动机是想在美国本土造成诸多麻烦，导致它无法再派遣部队到欧洲。这样，德军将不仅赢得海上战争，还将在欧洲战场上获胜，

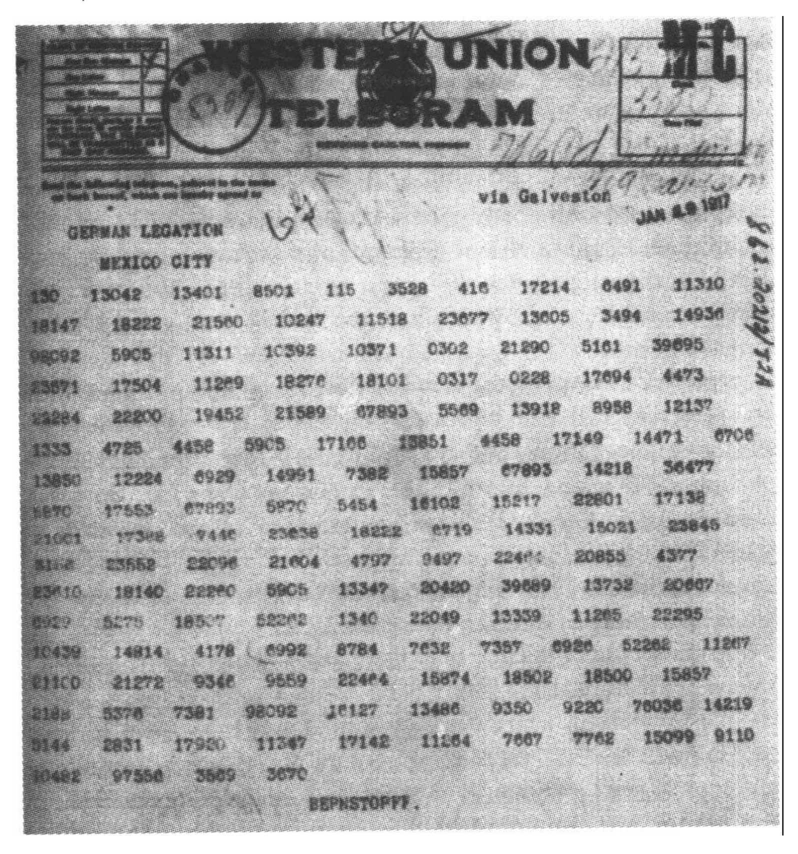


图 27:阿瑟·齐默尔曼

到时再从美国战场撤回部队。1月16日,齐默尔曼将他的提议压缩在一个电报里并交给德国驻华盛顿的大使,他然后再将电报转发给德国驻墨西哥的大使,再由这位大使递交给墨西哥总统。图28显示了加密后的电文。实际内容是这样的:

> 我们将在2月1日发动无限制潜艇战争。我们将尽力保持美国中立。否则,我们将向墨西哥提出联盟提议,条件如下:共同战争、共同和平,并有充足的经济支持,愿望是墨西哥能够收复得克萨斯、新墨西哥以及亚历桑那的领土。具体细节由你来处理。一旦美国决定要进入战争,你要秘密地将上述内容通知墨西哥总统,再附上一条建议即从他自身的利益出发,请日本也立即参战。请提醒墨西哥总统就是无限制的潜艇战将在几个月内就能迫使英国缴械,这已得到确认。
>
> 齐默尔曼

齐默尔曼不得不对他的电报进行加密,因为德国知道盟军正在截获所有跨大西洋的通讯。其实这也是英军的一个杰作,在一战第一天的凌晨,英国舰船"特尔康尼"号借着夜色的掩护悄悄靠近了德国的海岸,抛下锚,拉上了一捆海底的电缆,这些是德军跨大西洋的电缆——德军通往世界其他各地的通讯命脉。当太阳升起的时候,这些电缆已经全部被切断了,这次破坏活动目的是摧毁德军最安全的通讯系统,从而强迫德军通过不安全的无线电或其他国家的电缆来传送信息。齐默尔曼不得不经由瑞典发送了他的密文,作为备份还直接通过美国拥有的电缆发送。这两条路径都连到英国,这意味着齐默尔曼电报的内容很快会落到英国人手中,而事实也确实这样。



WESTERN UNION TELEGRAM

via Galveston

JAN 19 1917

GERMAN LEGATION

MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BERNSTORFF.

图 28:齐默尔曼送给德国驻华盛顿大使的电报,又转发给德国驻墨西哥大使。

这封加密电报立刻被送到“40 号房”即英国海军部的密码局,由于密码局最初的房间号是 40 号,所以以后就用“40 号房”来指密码局。“40 号房”是个奇怪的组合体,里面有语言学家、古文学者甚至动脑筋游戏迷,他们能够创造出密码破译学上最具才华的事迹来。例如其中的蒙哥马利教士,他是一位从事翻译德国神学

著作的天才。他曾破解了一个隐藏在一张邮政卡片里的密文。这张卡片是寄给苏格兰泰格汉巴奇镇国王路 184 号亨利·琼斯先生，卡片发自土耳其。因此亨利想，可能是现在是土耳其战俘发来的，但是亨利感到非常困惑为什么卡片是空的，而且地址也很奇怪，泰格汉巴奇镇其实很小，房屋并没有标号，也没有什么国王路。最终，蒙哥马利教士指出了邮政卡片中隐含的信息。其中地址是暗指圣经《列王记》第 18 章第 4 首诗："俄巴底亚带了 100 个先知，将 50 个藏在一个洞里，给他们面包和水。"亨利的儿子仅仅是安慰家里人他现在很好。当加密的齐默尔曼电报到达 40 号房后，由蒙哥马利和内格尔一起负责对其解密，内格尔曾是一位出版商。他们立刻发现他们正在处理一种只用在高层外交通讯的加密系统，所以时间有些紧急。解密绝非是件小事，但他们能利用以前其他类似加密电报的分析结果。几小时后这对密码破解者已经揭示出密文中的一些段落，足以看出其中的信息极具重要性。蒙哥马利和内格尔继续他们的工作，到了那天晚上，他们已经看清了齐默尔曼可怕计划的大体轮廓。他们认识到无限制潜艇战争是意味着什么，但同时他们也看见德国外交部长正鼓励向美国发动进攻，那很可能是激起威尔逊总统放弃中立。这封电报带有死亡性的威胁，但也有使美国加入盟军的可能性。

蒙哥马利和内格尔带着部分解密的电报，来到海军部情报门威廉霍尔主管那里，期望他将信息传给美国人，因而将他们拖入战争。然而，威廉霍尔上将只把这部分解密的信件放到保险柜里，鼓励他的密码破译师继续完成未加密的内容。他不愿递给美国一个不完整的解密电报，以免其中还有关键的地方没有被破译。同时他头脑里还有另外一个顾虑：如果英国给了美国解密的齐默尔曼电报，美国的反应可能是公开谴责德军的侵犯计划，那么德军将知道他们加密的方法已被破解。这将驱使他们发展更新更强大的加密系统，因而堵住了英国至关紧要的情报通道。但不管怎样，霍尔

知道德国潜艇的全面攻击将在两个星期后开始，这本身会足够引起威尔逊总统对德国宣战。假想期望的结果不管怎样都会发生的话，那么切断一个颇有价值的情报来源是没有意义的。

2月1日，按照德国皇帝的命令，德军发起了无限制海战。2月2日，伍德罗·威尔逊召开了一次内阁会议决定美国的反应。2月3日，他对国会宣布美国将继续保持中立，做一个和平使者，而不是参战者。这和盟军以及德国的预料相反。美国人不愿加入盟军就使得霍尔上将别无选择只有利用齐默尔曼电报。

蒙哥马利和内格尔第一次与霍尔见面的两个星期后，他们就完成了全部的解密。而且，霍尔发现有一种方法能使德国不会怀疑他们的安全性已经被破坏。他想到德国驻华盛顿大使冯·伯恩斯托夫首先会将信息作一些小的改动，再传给墨西哥的大使冯·埃克哈特，例如冯·伯恩斯托夫会先删掉电报上针对自己的指示，还要改变一下地址。然后冯·埃克哈特将这个修改后的电报解密后提交给墨西哥总统。如果霍尔设法弄到齐默尔曼电报的墨西哥版本，然后再将它公开在报纸上，那么德军将认为它是从墨西哥政府窃取的，而不会想到它是在去往美国途中被英国截获并破译的。霍尔联系了墨西哥的一个英国间谍，我们只知道他叫 H 先生，随后 H 先生潜入了墨西哥电报部门，在那里他能够获得任何他想要的，包括齐默尔曼电报的墨西哥版本。

霍尔将这个版本的电报递给了英国外交事务秘书长阿瑟·鲍尔弗。2月23日，鲍尔弗通知了美国大使沃特·佩奇，向他显示了齐默尔曼电报。后来佩奇称之为"一生中最震动的时刻"。四天后，威尔逊总统说道他见到了"雄辩的证据"，即德军正筹谋对美国的直接进攻。

电报被媒体公开，最终美国将不得不面临德军有侵犯企图这个事实。尽管美国民众之间几乎没有疑虑他们是否应该防御，可是美国政府还是有点担心这个电报是个英国人制造的一个骗局，

目的想确保美国卷入这场战争。然而关于真实性的问题很快就消失了，因为齐默尔曼公开地承认了他写过这封信。在柏林的一个新闻发布会上，没有人相逼，他简单的说“我不能否认它，这是真的”。



图 29：漫画《在他手中爆炸》，刊登在 1917 年 3 月 3 日的世界各大报纸上。

在德国外交部门开始调查美国人是如何获得齐默尔曼电报的。但他们被霍尔的计谋欺骗了，得出结论是“各种各样信息表明偷窃事件发生在墨西哥”。与此同时，霍尔继续分散人们对英国密码破译师的注意力。他在英国报纸上编了一个故事，批评自己的

组织没能截到齐默尔曼电报,这反过来导致一大批文章攻击英国的安全机构,同时表扬了美国人。

在年初的时候威尔逊说过把他的国家带入战争将是一种"对文明的犯罪",但是在1917年4月2日他改变了他的想法:"我建议国会宣布:近来德国政府的方针,实际上完全是在向美国政府和人民挑战,德国已经单方面正式接受了交战状态。""40号房"密码破译师一个简单的突破就挫败了一个预谋三年的外交政策。美国历史学家,《齐默尔曼电报》一书的作者巴巴拉·蒂奇曼做了下面的分析:

> 如果这个电报永远没有被截获或永远没有被公开,那么德国必然会做其他一些对我们有利的事情,但是时间已经很晚了,如果我们再延迟一下,盟军将被迫进入谈判。那样的话,齐默尔曼电报就改变了历史的走向。……齐默尔曼电报本身是历史长河中的一个小石子,但一个石子也能杀死歌利亚(圣经中被牧羊人大卫杀死的巨人,译者注),而这个石子则扼杀了美国人的幻想,即我们可以不管其他的国家自行其事。对国际事务来说,它是德国首相的一个小计策,而对美国人的生活来说,它代表着天真纯洁的结束。

密码编码学上的圣杯

第一次世界大战见证了一系列的密码破译家的胜利,齐默尔曼电报的破译使其达到了顶峰。自从19世纪的维热纳尔密码被破解以来,密码破译者一直领先于密码编码者。到了战末,当密码

编码师处于一种完全失望的状态时,美国的科学家取得了令人吃惊的突破。他们发现可以以维热纳尔密码为基础从中发展出一个新的、更牢固的加密形式。事实上,这个新密码确实能提供完美的安全保障。

维热纳尔密码最根本的弱点在于它的周期性。如果关键词是5个字母长,那么明文中每隔5个字母就使用同样的密码表来加密,如果密码破译师能确定关键词的长度,那么密文就可以被看作为由5个单字母替换密码组成的一个系列,每个都可以通过频度分析来破解。然而,试想一下如果关键词变得更长会出现什么结果。

假定有一篇1000个字母的明文用维热纳尔密码加密,我们要尝试破译它的密文。如果用来加密明文的关键词只有5个字母长,密码破译的最终一步将是对5组字母,每组200个进行频度分析,那是很容易的。但是如果关键词有20个字母,那么密码破译最后一步是对20组50个字母进行频度分析,难度将急剧增大。如果关键词是1000个字母,你将面临着对1000组每组仅1个字母进行频度分析,这是完全不可能的。换句话说,假如关键词(或关键词组)和信息内容一样长,那么由巴比奇和卡西斯基发展的密码破译技术将不起作用。

使用一个和明文一样长的密钥结果当然很好,但这需要密码编码者产生一个这么长的密钥。如果信息是几百个字母长,密钥也需要几百个字母。当然不能凭空创造这样的一个密钥,或许根据某个规则会比较好,比如说一首歌的歌词。或者密码编码师可以随意拿起一本鸟类鉴赏方面的书,从中随机选择一些鸟的名字以此来产生密钥。

在下面的例子中,我已经使用维热纳尔密码加密了一篇密文,使用的是和信息一样长的关键词组。所有前面讲述的密码破译技术都失败了。

关键词 ?
明　文 ?
密　文 V H R M H E U Z N F Q D E Z R W X F I D K

开始这个新的密码破译系统假定密文含有一些常见的单词，比如 the。然后我们随机将 the 放在明文的不同位点，如下所示，在推导什么样的关键字母需要来将 the 变成适当的密文。例如，如果我们假定 the 是明文的第一个单词，那么对于密钥的前三个字母它有什么暗示作用呢？密钥的第一个字母将 t 加密成 v。为了确定密钥的第一个字母，我们拿来一个维热纳尔方阵，从 t 列向下看直到字母 V，发现那一行是以 C 开头。对于 h 和 e 重复这样的过程，它们被分别加密成 H 和 R，最终我们得出密钥的前三个字母是 CAN。所有以上这些都基于事先的假定，即明文第一个单词是 The。我们将 the 放到其他的地方，再一次推出相应的密钥字母。（你可以参照图 9 来检查每个明文字母和密文字母之间的关系。）

关键词 C A N ? ? ? B S J ? ? ? ? ? ? Y P T ? ? ? ?
明　文 t h e ? ? ? t h e ? ? ? ? ? ? t h e ? ? ? ?
密　文 V H R M H E U Z N F Q D E Z R W X F I D K

我们已经在密文的任意三个位置测试了三个 The，对密钥的一些部位做了三个猜测。我们怎么知道这三个 the 中的任一个是否在正确的位置呢？我们认为关键词中含有一些敏感的单词，我们可以利用这些单词。如果某个 the 在一个错误的位置，那么根据它推出的密钥字母将是随机的。然而如果他在准确的位置，则密钥字母将有意义。例如第一个单词产生了关键字母 CAN（能够），这是令人兴奋的，因为它是个有意义的英文单词。很可能，这个 the 在准确的位置。第二个 the 产生 BSJ，这是个奇怪的辅音组

合,表明第二个 the 可能是错的。第三个 the 产生 YPT,这是个少见的音节,但是它值得进一步研究。如果 YPT 是密钥的一部分,那么仅有的可能性就是位于三个单词 APOCALYPTIC,CRYPT 和 EGYPT 以及他们的派生词中,我们怎么能发现这其中的某一个是密钥的一部分呢?我们可以将这三个单词分别插入到密钥中,再推出相应的明文,根据明文的意义来测试每一个候选单词。

```
关键词 C A N ? ? ? ? ? A P O C A L Y P T I C ? ?
明  文 t h e ? ? ? ? ? n q c b e o t h e x g ? ?
密  文 V H R M H E U Z N F Q D E Z R W X F I D K

关键词 C A N ? ? ? ? ? ? ? ? ? C R Y P T ? ? ? ?
明  文 t h e ? ? ? ? ? ? ? ? ? c i t h e ? ? ? ?
密  文 V H R M H E U Z N F Q D E Z R W X F I D K

关键词 C A N ? ? ? ? ? ? ? ? ? E G Y P T ? ? ? ?
明  文 t h e ? ? ? ? ? ? ? ? ? a t t h e ? ? ? ?
密  文 V H R M H E U Z N F Q D E Z R W X F I D K
```

如果某个候选单词不是密钥的一部分,它可能导致明文中出现一些无意义的片断。但是如果它是密钥的一部分,那么根据它产生的明文将有意义。对于 APOCALYPTIC 而言它产生的明文是最没有意义的。对于 CRYPT 它产生的明文是 cithe,这也是难以理解的。然而如果 EGYPT 是密钥的一部分,它将产生 at the,这个似乎有希望,可能代表单词 at the。

现在我们可以假定最具有可能性的是 EGYPT,或许密钥就是一些国家名。这将暗示我们第一个 the 对应的密钥那部分 CAN,可能是单词 CANADA 的开头部分。我们可以像 EGYPT 那样检验一下我们的假定,即 CANADA 是密钥的一部分:

关键词 C A N A D A ? ? ? ? ? ? E G Y P T ? ? ? ?
明　文 t h e m e e ? ? ? ? ? ? a t t h e ? ? ? ?
密　文 V H R M H E U Z N F Q D E Z R W X F I D K

我们的猜测似乎有点意义。CANADA 表明了明文是以 themee 开头,而它可能是 the meeting 的一部分。现在我们可以根据它推出明文中更多的字母,ting 在密钥中的相应部分原来是 BRAZ。显然这是指 BRAZIL。我们将以上组合起来得到密钥的大部分 CANADABRAZILEGYPT,据此得出如下的解密:the meeting is at the ????。

为了发现明文中的最后一个单词,即会议的地点,最好的方法是通过一个个测试所有可能的国家名,推出真正的明文。最后发现如果密钥最后一部分是 CUBA 的话,明文就是有意义的:"会议在码头开。"

关键词 C A N A D A B R A Z I L E G Y P T C U B A
明　文 t h e m e e t i n g i s a t t h e d o c k
密　文 V H R M H E U Z N F Q D E Z R W X F I D K

因此,一个和信息一样长的密钥并不一定安全。在上面的例子中它的不安全性主要是因为密钥是由有意义的单词组成。我们在明文中随机地插入单词 the,确定相应的密钥字母。我们可以判断单词 the 是否处在正确的位置,因为它产生的密钥字母看上去似乎是一些有意义单词的一部分。然后我们使用密钥中的这些片断来推出整个单词。反过来这些单词又给了我们更多的关于明文的信息片断,这些片断同样可以扩展成整个单词,依此类推。整个过程就是在信息和密钥之间反复尝试,其实这也是惟一可能的方法,因为密钥由一些有意义的单词构成,并且整个句子也有一定的结构。但是在 1918 年,密码编码师开始尝试使用没有任何结构特

表 9:维热纳尔方阵

Plain	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

征的密钥。结果产生一种无法破解的密码。

随着第一次世界大战接近尾声,美军密码研究机构头目约瑟夫·莫博涅少校引进了随机密钥的概念,即密钥不是由一些有意义的单词组成,而是一个随机的字母序列。他提议将这些随机密钥作为维热纳尔密码的一部分,那样可以提供一个空前高的安全保障。莫博涅系统的第一步是编辑一本厚的由几百页组成的小册子,每一页都是由随机排列的字母组成并作为一个独一无二的密钥。这个小册子将有两本,一本给发送者,另一本归接收者。加密

一个信息时,发送者将使用小册子的第一页作为密钥对明文应用维热纳尔密码加密,图 30 显示了这样一种小册子其中的三页(真的小册子每页含有数百个字母),在它的下面是一段根据第一页随机密钥加密的信息。接收者使用同样的密钥即可容易地解开密文。

一旦信息被成功地发送、接收和解密,发送者和接收者都同时销毁已用作密钥的那一页,因此这个密钥再也不会被第二次使用,当需要加密另一条信息时,那么小册中下一页的随机密钥就被使用。同样,在使用完之后它也被销毁。由于每个密钥都使用而且仅使用一次,所以这个系统就称作一次性便笺密码。

Sheet 1	Sheet 2	Sheet 3
P L M O E	O I W V H	J A B P R
Z Q K J Z	P I Q Z E	M F E C F
L R T E A	T S E B L	L G U X D
V C R C B	C Y R U P	D A G M R
Y N N R B	D U V N M	Z K W Y I

关键词 P L M O E Z Q K J Z L R T E A V C R C B Y
明　文 a t t a c k t h e v a l l e y a t d a w n
密　文 P E F O G J J R N U L C E I Y V V U C X L

图 30:一次性便笺密码

一次性便笺密码克服了以前密码的所有弱点。试想如果有这样的信息 at tack the valley at dawn(凌晨攻击山谷)已经被加密(图 30),通过无线电传送并被敌人截获,密文被交到了敌方密码破译师手中,然后该密码破译师试图破译它。遇到的第一个障碍将是随机密钥没有重复的字母组合,因此使用巴比奇和卡西斯基的方法不能破解一次性便笺密码。敌方密码分析师也可以采用第

二种方法，就像我们刚才破译前面的那段信息一样，将单词 the 放在不同的位置。如果密码破译师试着将 the 放在信息的开头，实际是不对的，然后得出密钥中相应的片断是 WXB，这是个随机的字母序列。如果密码破译师恰好将 the 放在信息的第七个字母开头，虽然碰巧是对的，但是得出的密钥相应片断是 QKJ，这也是个随机的字母组合。换句话说，密码破译师不能判断这个试验单词是否处在了正确的位置。

实在没有办法，密码破译师可能会考虑使用无穷搜索所有可能密钥的方法。这个密文含有 21 个字母，因此密码破译师知道密钥也有 21 个字母。这意味着大约有 5×10^{29} 个可能的密钥等待去测试，无论是人力还是机械运算这都是完全不可能的。即使密码破译师能够测试所有可能的密钥，还是存在一个更大的问题需要去克服。通过检查每一个可能的密钥，密码破译师当然会发现真正的信息，但是也同样会得到每一个错误的信息。例如下面的密钥用在同样的密文上则产生一个完全不同的信息（“日落前守住山头”）。

关键词 M A A K T G Q K J N D R T I F D B H K T S
明　文 d e f e n d t h e h i l l a t s u n s e t
密　文 P E F O G J J R N U L C E I Y V V U C X L

如果所有不同的密钥被测试完，每一个有意义的由 21 个字母组成的信息都会产生，密码分析师将不能辨别究竟哪一个才是真正的原信息。如果密钥是由一些单词或词组组成，那么就不会出现这个问题，因为在那种情况下，无意义的密钥不会产生有意义的信息，而有意义的信息只能由有意义的密钥产生。

一次性便笺密码的安全性全在于密钥的随机性。这种密钥也使密文具有了随机性，如果密文是随机的，那么它就没有任何模

式,没有任何结构,密码破译师也就没有任何突破的地方。事实上,可以从数学上证明,密码破译师是无法破解一条由一次性便笺密码加密的信息。换句话说,一次性便笺密码不仅仅被认为是无法破解的,就像19世纪维热纳尔密码一样,它真的是绝对地无法破解,绝对地安全。一次性便笺密码提供了一个安全的保证:密码编码学的圣杯。

终于,密码编码学者发现了一个无法破解的加密系统。然而,完美的一次性便笺密码并没有结束人们对安全的顾虑:事实的真相是这种密码很难被使用。尽管在理论上,它是完美无缺的,但实际操作起来却存在着很大缺陷,因为该密码有两个根本的难点。首先制造大量的随机密钥实际上是很困难的。一个军队在一天内能交换成百的信息,每个含有上千的字符,无线电操作员每天需要的密钥将达上百万个字母。提供如此多的随机字母序列将是一件巨大的工作。

过去,一些密码编码者认为他们可以通过在一台打字机上随意敲击,来产生大量的随机密钥。然而这样的话,打字员将会有一种习惯就是先用左手敲击一个字符,再用右手敲击一个字符,这样往复下去。这虽然是一种快速的产生密钥的方法,但是产生的序列是有结构的,不再具有随机性。如果一个打字员在键盘的左边击了字母D,那么下一个字母将是可以预测的,至少它可能是在键盘的右边。如果一次性便笺密码真的是随机的,那么位于左边键盘的一个字母,它的下一个字母大约有一半的几率也是位于键盘的左边。

密码编码者开始就认识到这种密码需要消耗大量的时间、精力和财力去产生一个随机密钥。最好的随机密钥应该利用自然的物理过程来创立,例如放射性即具有真正随机的行为。密码编码者可以在工作台上放置一块放射性物质,再用盖革计数器来测定它的放射能。有时候放射能连续不断地发生,有时候发射之间有

所延迟，两次发射之间的时间是不可预测的，具有随机性。密码编码者可以在盖革计数器上连接一个显示屏，首先显示屏上会以一定的速率循环显示字母表中的字母，一旦检测到放射屏幕会暂时冻结。此时屏幕上显示的字母就可以作为密钥中的一个字母。然后显示屏重新开始循环直到下一次放射后停止，屏幕上的字母就加到密钥中，依次类推。这种处理可以保证产生一个真正随机的密钥，然而这对于每天进行的密码编码来说它同样是不实际的。

即使你能产生足够的随机密钥，第二个问题又来了，就是如何分发它们。试想战场上成百的无线电操作员处在同一个通讯网络中。要想开始工作，每个人必需有完全一样的一次性手册。然后当新的手册发行后，它们必须同时分发到每个人的手中。最后每个人必须在步调上保持一致性，以确保他们在特定时间使用的是手册上的同一页。一次性手册的广泛使用将使战场上充满了信使和持书人。敌方只要捕获一套这样的密钥，那么整个通讯系统就瘫痪了。

或许有人会认为使用一次性手册循环会好些，因为这减少了密钥的制作和分发，但是这却犯了密码编码学上最忌讳的毛病。重复使用同一个一次性手册将使敌方密码破译师更加容易地破译信息。但是关键的问题是使用一次性便笺密码是不能指望有什么快捷途径，发送者和接收者对每个信息都必须使用一个新的密钥。

一次性便笺密码只有当通信双方需要绝对的安全保障，并能够承受制造和秘密发送密钥时所需的巨大消耗，才具有实际的意义。例如，在俄罗斯和美国总统之间的热线就是由一次性便笺密码来保障安全。

一次性便笺密码理论上的完整和应用上的缺陷意味着莫博涅的思想永远不能用在激烈的战场中。第一次世界大战过后，密码编码者在经历了各种失败后，继续寻找一种实用的加密系统想用在下一次战争中。幸运的是，密码编码者不久就取得了一个突破，

能够在战场上重建秘密通讯。为了加强他们的密码,密码编码师不得不放弃了传统的笔和纸的方法,而采用一种最先进的技术来混乱信息。

密码机的发展:从密码盘到恩格玛密码机



图 31:"密码表",美国内战时期北方军队使用的密码盘。

最早的密码机器是密码盘,是 15 世纪由意大利建筑师利昂·阿尔伯提发明,利昂·阿尔伯提也是多字母替换密码创始人之一。他使用两个铜盘,一个比另一个稍大,在每个盘的边缘刻上了 26 个字母。将小盘子放在大盘子上,中间用一根针作为轴心。他制造的东西有点像图 31 所示的密码盘。两个盘碟可以相互转动,上

面字母即可以处于不同的相对位置,事实上这就像一个简单的恺撒移位密码可以用来加密一条信息——外面的盘代表明码表,里面的盘代表密码表。明文信息中的每个字母能在外盘中寻找到,其内盘对应的字母即可组成密文。要发送一个用恺撒5位移位密码加密的信息,只需简单地旋转密码盘使外盘的A对着内盘的F,然后再用这个设置好的密码盘加密。

虽然密码盘是一个非常简单的装置,但它确实简化了加密过程,这使它存在了近五个世纪。图31所示的这个密码盘是用在美国内战时期,图32显示的密码盘叫“密码表”。美国早期有一个无线电节目叫“午夜队长”,其中有一个著名英雄就使用这个密码盘,听众可以写信给节目负责人索取他们自己的“密码表”。节目有时会在结束的时候留下一个“午夜队长”的密文,忠实的听众可以使用“密码表”来破译这个密文。密码盘可以被认为是个“扰频器”,将每个明文字母变成其他什么东西。

到目前为止描述的操作模式是非常直接的,其产生的密码破解起来相对比较容易,但是密码盘可以有更复杂的用途。它的发明者阿尔伯提提出,在加密的过程中可以不断改变轮盘的设置,那样实际上就产生多字母替换密码而不是简单的单字母替换密码。例如,阿尔伯提用他的轮盘来加密单词goodbye(再见),关键词是LEON。他先根据关键词的第一个字母来设置他的轮盘,将外盘的A指向内盘的L。然后他可以加密信息的第一个字母g,找到g在外盘上的位置记下内盘上对应的字母是R。要加密信息的第二个字母,则根据关键词的第二个字母重新设置轮盘,将外盘的A指向内盘的E。然后找到o在外盘上的位置,即可发现内盘对应的字母是S。接下来根据关键词字母O继续上述的加密过程,然后是N,再后又回到L,如此反复。阿尔伯提实际上已经用他的名字作关键词使用维热纳尔密码加密了一段信息。用密码盘加密与用维热纳尔方阵加密相比,它提高了加密速度,减少了错误。



图 32:“午夜队长”使用的密码表外盘指示明文字内盘的密文用数字表示。

像这样使用密码盘加密的一个重要特色就是在加密的过程中,它能改变它的混乱模式。尽管这高一层的复杂性使得密码更难破解,但这并不能使它无法破译,因为我们只不过是在处理一种机械化的维热纳尔密码,而维热纳尔密码已经被巴比奇破解了。在阿尔贝提以后500年,他的密码盘已经演变成了一个更加复杂的装置,产生了新一代的密码,一种比以前使用过的任何密码都难破解的加密系统。

1918年,德国发明家阿瑟·谢尔比斯和他的好朋友理查德·里特建立了谢尔比斯 & 里特 公司,这是个充满创新的工程公司,涉及到许多领域,从涡轮机到热枕垫几乎无所不做。谢尔比斯负责研究和开发,经常寻找新的设计。他的一个特别计划就是想替换一战时使用的缺陷多多的密码编码系统,利用一种融进20世纪

技术的加密方式来代替笔纸密码。在汉诺威和慕尼黑学完电气工程后,他发明了一个密码编码装置,本质上它仅仅将阿尔贝提密码盘电子化。谢尔比斯的发明被称为恩格玛(谜)机,当时或许没有认识到它将成为历史上最厉害的加密系统。

谢尔比斯的恩格玛机的每个部件都充满了创造性,谢尔比斯再将这些零件组装成一个特别复杂的密码机。然而,如果我们将这个机器拆开再一步步组装起来,那么里面的原理就变得一清二楚了。谢尔比斯的发明基本上由三大部件组成,它们之间通过电线连接起来,分别是:一个键盘,用来输入每个明文字母;一个扰频器,用来将每个明文字母加密成相应的密文字母;一个显示板,由各种灯构成用来显示密文字母。图 33 是该机器的简易装置图,仅使用了 6 个字母。加密一篇明文时,操作员只需在键盘上敲击准确的明文字母,每次敲击都会发送一个电脉冲经过扰频器,在另一边的灯板上相应的明密文字母就发亮。

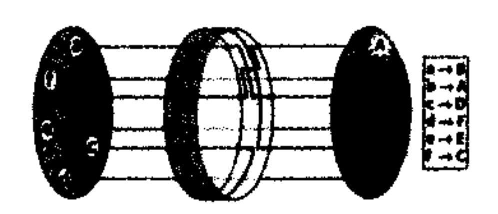


图 33:这是一幅六字母恩格玛密码机的简图,其关键部件是扰频器。若按键盘上的字母 b,电流就会顺着线圈通过扰频器,灯泡 A 就会闪亮,简言之,b 被加密为 A,右面的方框显示六个字母的密码表。

扰频器是个厚厚的橡胶盘,上面穿过许多电线,它是整个机器的最重要部件。在键盘这一边,电线从 6 个点穿入扰频器,在里面经过一系列的曲折分别从另一端出来。扰频器中内部的电线决定了明文字母如何被加密。例如,在图 33 里,线路表明了:

输入 a 将使 B 显亮，意味着 a 已经被加密成 B；
输入 b 将使 A 显亮，意味着 b 已经被加密成 A；
输入 c 将使 D 显亮，意味着 c 已经被加密成 D；
输入 d 将使 F 显亮，意味着 d 已经被加密成 F；
输入 e 将使 E 显亮，意味着 e 已经被加密成 E；
输入 f 将使 C 显亮，意味着 f 已经被加密成 C。

信息 café 将被加密成 DBCE。通过这样基本的设置，扰频器本质上是定义了一个密码表，从这个意义上它可以用来实现一个简单的单字母替换密码。

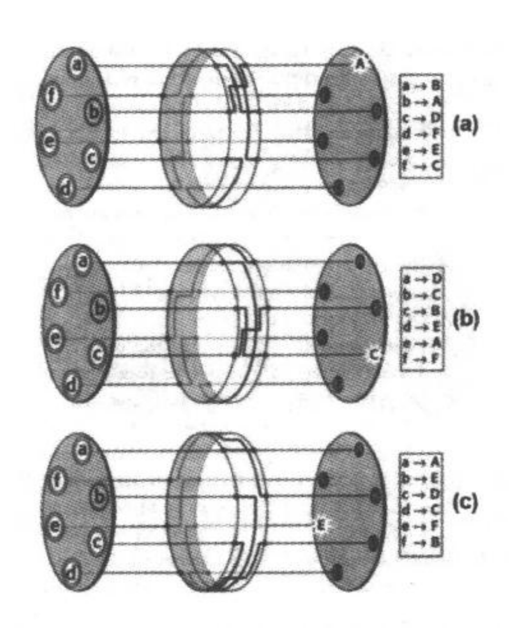


图 34：每次按键盘上的一个字母，扰频器就会转动一格，字母就随即被加密，在图(a)中，扰频器将 b 加密为 A，在图(b)中，扰频器将 b 加密为 C，在图(c)中，扰频器转到另一个位置，将 b 加密为 E。四次加密后，扰频器返回到原来的位置。

然而,谢尔比斯的想法却不是这么简单,事实上扰频器在每次加密一个字母后会自动地旋转 1/6 圈(对于完整的 26 个字母表则旋转 1/26 圈)。图 34(a)所示的是和图 33 一样的结构。这一次同样敲入字母 b 将显亮字母 A,但是在这一次完了之后,扰频器会自动地旋转 1/6 圈到了图 34(b)的位置。再次输入字母 b 将显亮一个不同的字母 C。紧接着扰频器会再次旋转,到了图 34(c)的位置。这次输入字母 b 将显亮 E。连续输入六次 b 将产生密文 ACEBDC。换句话说,在每次加密过后,密码表都会改变,因此对字母 b 的加密也在不断改变。有了这种旋转设置,扰频器本质上就定义了 6 个密码表,对比来说它可以用来实现一个多字母替换密码。

扰频器的旋转是谢尔比斯设计中一个最重要的特色。但是这台机器却有一个明显的弱点。输入 b 六次后将使扰频器回到原始状态,一次次输入 b 将重复同样的加密模式。因此密码编码师必须避免这种重复,因为它导致产生的密文具有规则性和结构性,这是普通密码的一个通病。但这个问题可以通过引入第二个扰频器来缓解一下。

图 35 是具有两个扰频器的密码机示意图。由于扰频器的三维结构很难表示,图 35 只用了二维结构来表示。每当一个字母被加密,第一个扰频器就旋转一个位置,或者以二维图来说每根线都向下移一个位置。相反第二个扰频器在大部分时间都保持不动。只有当第一个扰频器旋转一圈后,第二个扰频器才移动一次。第一个扰频器上装有一个齿轮,只有这个齿轮到了一定位置时,它就带动第二个扰频器移动一个位置。

在图 35(a)里,第一个扰频器即将带动第二个扰频器转动。输入并加密一个字母后,情形如图 25(b)所示,其中第一个扰频器已经移动了一个位置,第二个扰频器也被带动旋转一个位置。输入和加密第二个字母,第一个扰频器将再次移动一个位置,见图 35(c),但这次第二个扰频器保持不动。第二个扰频器直到第一个

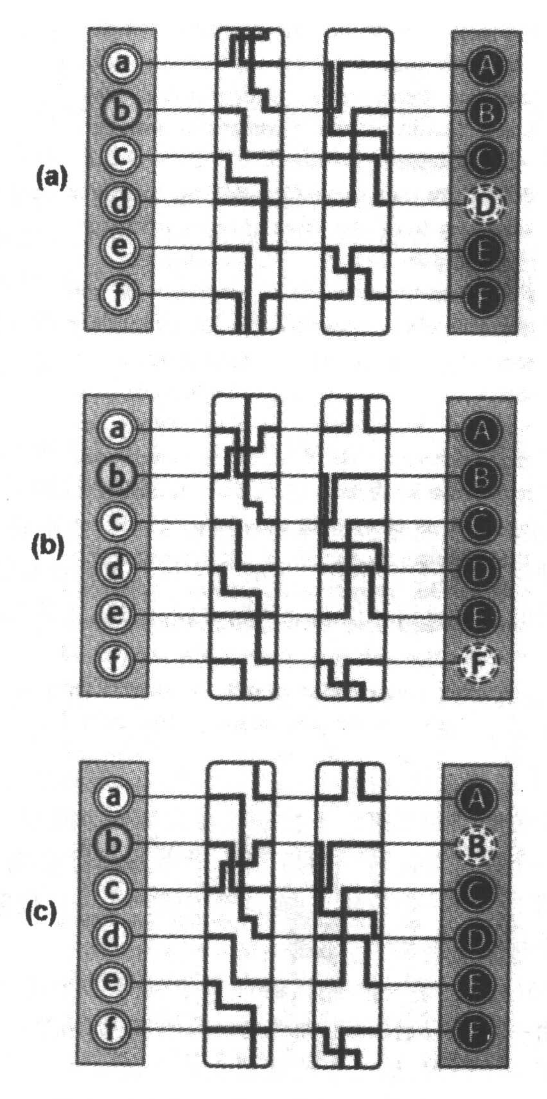


图 35:为具有二个扰频器的密码机示意图。

扰频器旋转一圈之后再移动一次，这还需要5次的加密。这种装置就像一个汽车里程表——代表单数英里的转轮会快速的旋转，当它完成一圈后到达“9”时，就会带动代表10位数英里的转轮转动一次。

加入第二个扰频器的好处，在于加密的模式直到第二个扰频器完成一圈旋转后才出现重复，这需要第一个扰频器完成6次的转圈，或者需要加密6×6即36个字母。换句话说，两个扰频器能组合成36种不同的设置，相当于在36个密码表之间来回切换。对于一个有26个字母的完整密码表来说密码机将在26×26，即总共376个密码表之间切换。

因此，通过组合扰频器（有时候称作转轮）产生的密码机可以连续在不同的密码表之间切换。操作员输入一个特定的字母后，根据转轮的组合方式，这个字母可以通过几百个密码表中的任一个来加密。然后扰频器组合发生变化，使得下一个输入机器的字母根据一个不同的密码表来加密。而且，由于扰频器的移动都是自动的，并且又是电动的，以上所有过程都可高效准确地进行。

在详细解释谢尔比斯本人如何使用他的加密机之前，我还要描述一下恩格玛机的另外两个元件，如图36所示。首先，谢尔比斯的标准加密机具有第三个扰频器，使其更加复杂——对于一个完整的字母表来说，这三个扰频器就能提供26×26×26即总共17576种不同的扰频器组合。其次，谢尔比斯还加了一个反射器。反射器有点像扰频器，因为它也是个橡胶盘，内部有电线。但这两者也有不同的地方，因为它不旋转，而且线路是从一面进去还从同一面出来。有了这个反射器，当操作员输入一个字母后，即发出一个信号经过三个扰频器，当反射器接收到第三个扰频器送来的信号后再将这个信号反射再次经过这三个扰频器，但是沿着一个不同的路径。例如，按照图36的设置，输入字母b将发出一个信号经过三个扰频器进入反射器，在反射器里通过回路又返回来通过

这三个扰频器最后到达字母 D。图 36 中信号实际并没有经过键盘,而是直接传向了灯板。乍看上去,反射器附加在机器里似乎没有意义,因为它的静态特性意味着它不能增加密码表的数量。然而,当我们明白这种机器究竟是如何来加密和解密一条信息时,它的优点就变得清楚了。

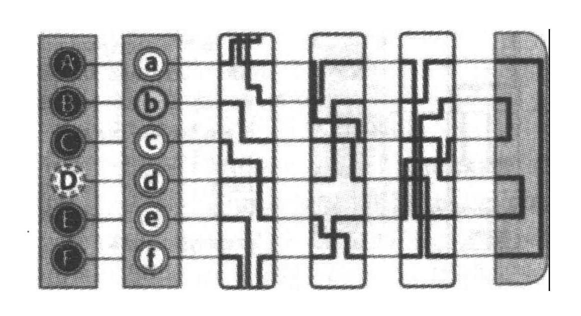


图 36:谢尔比斯设计的恩格玛机示意图

一个操作员希望发送一条秘密信息。在加密开始前,该操作员必须首先旋转扰频器到一个特定的开始位置。总共有 17576 种可能的组合,因此有 17576 种可能的开始位点。扰频器最初的设置将决定信息是如何加密的。我们可以将恩格玛机想像成一个普通的密码系统,最初的设置决定着加密的具体细节。换句话说,最初的设置提供了密钥。最初的设置通常被记录在一本密码簿中,里面列出了每天使用的密钥,在某个特定通讯网络中每个人都有这样的簿子。分发这个簿子需要时间和人力,但是由于每天只需要一个密钥,那么每个密码簿可以有 28 个密钥,这样即可每 4 个星期分发一次。作为比较,如果一个军队使用的是一次性便笺密码,那么每个信息都需要一个新的密钥,密钥的分发也是一件更为艰巨的工作。一旦根据密码簿的每日要求扰频器被设置好,发送

者就可以开始加密。他输入信息中的第一个字母,观察灯板上哪个字母被显亮,并记录下来作为密文的第一个字母。然后当第一个扰频器自动地移动一个位置后,发送者就输入信息的第二个字母,依次下去。一旦他产生了一篇完整的密文,就交给无线电操作员将它传送到接收者手中。

为了破译这个信息,接收者需要有一台同样的恩格玛机和一本同样的密码簿,其中含有当天的扰频器最初设置。他根据密码簿设置好机器,逐个输入密文字母,灯板上显示出明文。也就是发送者输入密文产生明文,而接收者输入明文产生密文——加密和解密是两个互为镜像的过程。解密的简便就得益于反射器。从图36中我们可以看出如果我们输入字母b,沿着电路走向我们将回到字母D。同样,如果输入字母d,沿着电路我们将回到字母B。这个机器能将明文字母加密成密文字母,但只要处于同样的设置,它也能将同样的密文字母变回明文字母。

很明显密钥以及含有密钥的密码簿必须永远不能落入敌方的手中。敌方是非常有可能截获一台恩格玛机,但是不知道加密时的最初设置,他们是不容易破译一条截获的信息。假如没有密码簿,敌方密码破译师就必须采用检验所有可能密钥的方法,这就意味着要尝试17576种可能的扰频器设置。孤注一掷的密码破译师会先将扰频器设置在一定状态,再从截获的密文中选取一小段输入机器中,观察输出的结果有没有意义。如果没有意义再变换一种扰频器观察设置结果。如果他每分钟能检验一种扰频器组合并且日夜工作,那么检查完所有的设置将花费2个星期的时间。如果敌方派12个人同时工作,那么一天内就能检验完所有的设置。因此谢尔比斯决定对他的发明作一些改进以提高安全性,于是他增加了最初设置的可选数量,因而增加了可能密钥的数目。

他本来可以增加更多的扰频器(每个新增的扰频器可以将密钥的数量提高26倍)来提高安全性,但是这样会增加恩格玛机的

尺寸。相反，他添加了另外两个特色进去。首先，他简单地使扰频器可以移动即可以内部变动。例如第一个扰频器可以被移到第三个位置，第三个扰频器可以相应移到第一个位置。扰频器的相对位置影响着加密过程，因此加密和解密时需要确切的位置关系。三个扰频器共有 6 种排列方式，因此这个特性使得密钥的数目或者说初始设置的数目提高了 5 倍。

第二种新的特性是谢尔比斯在键盘和第一扰频器之间插入了一个插件板。插件板允许发送者插入连接器，它能在字母进入扰频器之前先交换字母的位置。例如，用一个连接器连接插件板中的 a、b 槽，这样当密码编码者想加密字母 b 时，发出的电信号所走的实际路径和以前字母 a 所走的路径一样。恩格玛机操作员有 6 个连接器，也就是能交换 6 对字母，剩下 14 个字母没有被交换。通过插件板交换的字母也是机器设置的一部分，因此必须在密码簿中明确地表明出来。图 37 是带有插件板的机器的示意图。因为该图仅表示了 6 个字母，所以只有一对字母 a 和 b 被交换了。

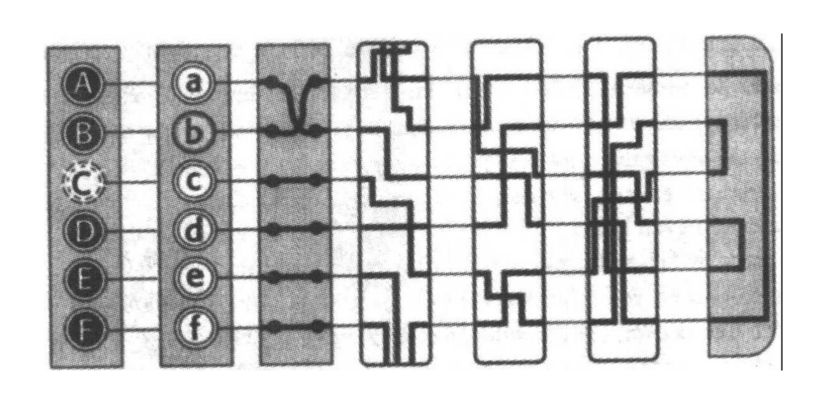


图 37：带有插件板密码机的示意图

谢尔比斯设计中还有另外一个特色，被称为“环”，我们还没有

提及它。尽管“环”确实对加密有一定的影响，但它是整个恩格玛机中的最不重要的部分，因此我决定在这里就忽略它不再讨论。现在我们知道了谢尔比斯的恩格玛机所有主要部分，我们将插件板连接器的数目和扰频器可能组合的排列综合起来，来算一算密钥的数目究竟达多少。下面列出了机器的每个参量以及各自相应的概率数：

扰频器的定位：3个扰频器每个有26个状态，因此将有

$26\times26\times26=17576$ 种设置。

扰频器排列：3个扰频器（1，2和3）共有6种不同的排列方式：

123，132，213，231，312，321。

插件板：在26个字母中任意交换6对字母，那么连接方式的数目是巨大的：100391791500

综合：将以下三个数相乘即得密钥的总数目

$17576\times6\times100391791500\approx10^{16}$

只要发送者和接收者之间在插件板的连接器、扰频器的次序以及各自的状态上保持一致，那么他们将很容易地加密和解密某条信息。但是，如果一个敌方拦截员不知道密钥的话，要想破译密文他将不得不检验 10^{16} 种可能密钥中的每一个。这种情况下，对于一个固执的密码破译者来说，即使他能每分钟检查一种设置，他也将需要比宇宙年龄还长的时间去检查每一个设置。

到现在我们发现恩格玛机中对密钥数量贡献最大的来自插件板，你可能会想到为什么谢尔比斯还要这么麻烦地使用扰频器。事实上，如果单有插件板本身，它提供的密码将是微不足道的，因为它形成的密码就是单字母替换密码，而且只能交换12个字母。插件板的问题在于一旦加密开始，交换就不会再改变，因此它产生的密文可以用频度分析来破解。而扰频器虽然对密钥数量的贡献不大，但它的设置在加密过程中不断地变化，这使得产生的密文不

能通过频度分析来破译。谢尔比斯将扰频器和插件板巧妙的组合起来,防止了别人使用频度分析来破解它产生的密文,同时也具有了庞大数量的密钥可能。

谢尔比斯在 1918 年为他的装置第一次申请了专利。他的密码机包装在一个紧凑的盒子中,尺寸是 34×28×15cm,重量却达到 12 公斤。图 39 所示的是一个恩格玛机,它的盖子已经打开,准备使用。我们可以看到其中的键盘,从这可以输入明文字母。键盘的下面是插件板,通过插件板可以交换超过 6 对的字母,因为这个恩格玛机已经在我们先前介绍的基础之上做了一些改进。图 40 所示的恩格玛机的外壳已被打开,我们可以看见里面更多的内容,特别是三个扰频器。

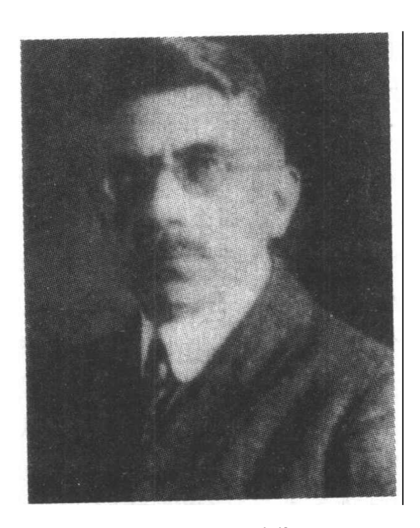


图 38:谢尔比斯


Q W E R T Z U I O
A S D F G H J K
P Y X C V B N M L
Q W E R T Z U I O
A S D F G H J K
P Y X C V B N M L

图 39:一部军用密码机

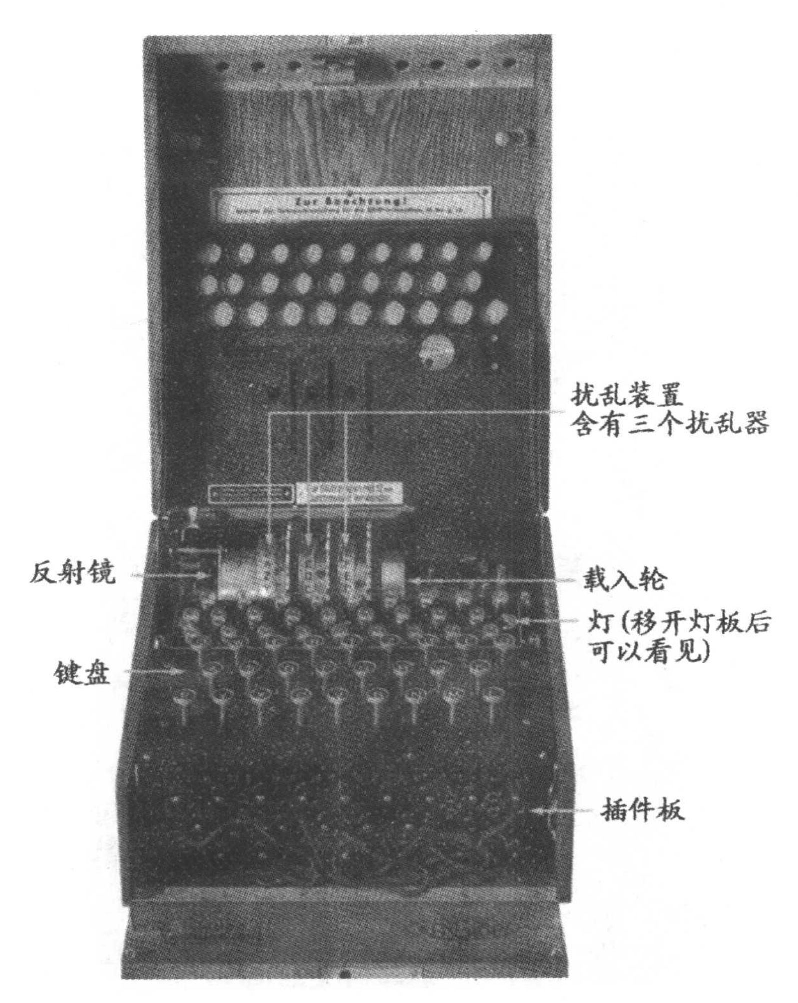


图 40:一部军用密码机的外壳已被打开,显现出三个扰频器。

谢尔比斯相信恩格玛机是无法攻破的,它强大的编码能力将产生巨大的需求量。他同时在军事和商业活动上开拓市场,并根据不同的需求提供各种不同的型号,他为商人提供了一个基本型的恩格玛机,而为外交部门则专门提供了一个豪华的外交型恩格玛机,该型号没有了灯板而取代以打印机。每个恩格玛机以今天的价格将达到 20000 英镑。

然而遗憾的是,该机器昂贵的价格使许多有意愿的购买者望而却步。商人说,他们用不上恩格玛机的高安全性,而谢尔比斯则认为他们不能没有它。他说一条关键的信息如果被商业对手截获,那代价可能就是整个公司的破产,但是很少有商人注意到他。德国军方同样也是没有太大热情,他们似乎已经遗忘了在一战中使用的不可靠的密码所带来的损失。例如,他们被人家蒙骗到相信齐默尔曼电报是在墨西哥被美国间谍窃取,因此他们就把失败归咎于墨西哥的安全系统。他们仍然没有意识到电报是被英国人截获并解密,齐默尔曼计划的破灭,实际上是德国密码编码术的一次惨败。

并不是只有谢尔比斯一人感到沮丧。在另外三个国家也有三个其他的发明者,他们各自几乎同时产生了基于旋转扰频器的密码机想法。1919 年荷兰人亚历山大·科恩发明了 10700 型密码机并申请了专利,但他没有成功地将他的转轮机市场化,最终在 1927 年,他卖掉了他的专利权。在瑞典,阿维德·达姆恩也申请了一个相似的专利,但是直到 1927 年他去世后,也还没能为他的发明找到市场。在美国,发明家爱德华·赫伯恩对他的发明抱有十足的信心,这个取名为无线斯芬克斯的发明给他带来的失败,却是所有人中最大的。

在 20 年代中期,赫伯恩斥资 38 万英镑建立一座工厂,但不幸的是这个时期美国人的思想正从偏执主义向开放主义转变。在战后的前 10 年,美国政府建立了美国人自己的密室,一个由 20 多位

密码破译师组成的高效的密码局，并由当时才华横溢的赫伯特·亚德利领导。后来亚德利写道："密室相当隐蔽，终日上锁，有门卫把守。虽然窗户是紧闭的，窗帘是拉上的，但它的千里眼能渗透到华盛顿、东京、伦敦、巴黎、日内瓦、罗马的秘密会议室。它的顺风耳能捕获世界外国首都的最微弱的声音。"美国在 10 年内解决了 4500 个密码问题，但是等到赫伯恩建造工厂的时候，赫伯特·胡佛被选为总统，他试图将整个世界带入一个在国际事务上相互信任的新时代。他解散了密室，他的国务卿亨利·斯廷森宣布"绅士们不应该偷看其他人的邮件"。如果一个国家认为偷看别人的信息是错的话，那么它也会开始认为别人也不该看自己的信息，这样的话就看不出密码机存在的必要。赫伯恩前后总共只卖出了 12 台机器，而且总价钱仅有 1200 英镑。1926 年，他被不满的股东告上法庭，最终以侵犯加利福尼亚公司安全法而判有罪。

然后万幸的是，德国军方思想最终开始动摇，开始考虑赫伯恩恩格玛密码机的价值，这还得感谢两个英国文件。第一个来自温斯顿·丘吉尔，他在 1923 年出版的《世界危机》里面，详细说明了英国人是如何得到有价值的德军密码材料：

> 1914 年 9 月初，德军轻型巡洋舰曼德伯格号在波罗的海沉没。几小时后一位溺死的德国军官的尸体被俄国人捞起，他的胸前紧紧抱着一本德国海军密码和信号册以及关于北海相关地区缩略地图。9 月 6 日，俄国海军武官前来见我，告诉我这一切。他刚收到从彼得格勒发来的情报，以及俄国海军部利用这本密码和信号册能够得到的一部分德国海军信息。俄国人认为英国海军部作为海上领导力量应该拥有该书和地图。如果我们派一艘舰船到亚历山大罗夫港，俄国军官将负责把这些材料带到英国。

这些材料有效地帮助了英国海军部密码局破解德军加密的信息。终于,几近10年后,德军才认识到他们通讯安全上的巨大失败。1923年,英国皇家海军也出版了关于第一次世界大战的官方历史资料,里面也提到对德军通讯的截获和分析使得盟军具有明显的优势。英国情报部门所取得的令人骄傲的成就,使那些负责德国安全防卫的官员面色全无,他们最后不得不承认"德军舰队司令部的无线电信息被英国截获并解密,一直在和英国舰队司令部打明牌"。

德军曾召开了一个研讨会,讨论如何在密码编码上避免发生一战时的惨痛失败并得出结论恩格玛机是最好的解决办法。1925年,谢尔比斯开始大量生产恩格玛机,第二年恩格玛机就进入军事部门服务,然后又被政府部门采用,接着又进入地方机构如铁路系统中。这些恩格玛机和谢尔比斯先前卖给商业组织的机器不同,因为其中的扰频器内部线路作了改动。因此商业恩格玛机的拥有者并不能完全了解政府和军事部门恩格玛机的结构原理。

在接下来的20年里,德国军方购买了近20000台恩格玛机。谢尔比斯的发明为德国军方提供了世界上最安全的密码编码系统,二次世界大战爆发后,他们的通讯受到空前安全的加密系统的保护。曾经一度时间,恩格玛机似乎成了战场上一个至关紧要的角色,甚至能带给纳粹决定性的胜利。然而它最终也成了希特勒垮台的一个因素。谢尔比斯过早地去世了,他也没能见证他的密码系统所经历的成功与失败。1929年,当他驾着马车外出时,突然马车失去控制撞到了墙上,谢尔比斯于5月13日,因内脏损伤而离世。

第四章 破解恩格玛

在第一次世界大战后的第二年，40号房的英国密码破译员仍继续监听德国的通讯。在1926年，他们截取到让人十分困惑的一段讯息。谜语出现了，但40号房破解密码的才智已随着密码机数量的增加而迅速下降。美国人和法国人也尝试解开这个密码谜，但他们的努力也以失败告终，人们很快就放弃了破解这种密码的希望。因此，当时的德国拥有了世界上最安全的通讯方法。

盟军的密码破译员们放弃破解恩格玛码希望的速度与他们在20年前第一次世界大战时对密码破解的坚持不懈，形成鲜明对比。在那时，面对战败的前景，盟军的密码破译员们夜以继日地工作以破译密码。这样看来，似乎恐惧是推动密码破译的主要动力，而所谓的患难也似乎成为密码破译成功的原因之一。与此类似，19世纪末，面对德国日益强大的力量，正是恐惧和患难，激励着当时的法国密码破译员。然而，在第一次世界大战后，盟军不再惧怕任何国家。德国已因战败而削弱了国力，盟军处于支配地位，因此，他们似乎丧失了破译密码的热情。盟军的密码破译员们在数量上减少了，素质也大不如前。

可是，一个国家是承担不起松懈疏忽的代价的。第一次世界大战后，波兰重新成为独立国家，它始终关注着各种对新建政权的

威胁。在东边,苏联正野心勃勃地传播共产主义;在西边,德国正绝望地想重新获得一战后划给波兰的土地。前狼后虎,波兰人不顾一切地搜寻有价值的信息,为此,他们建立了新的密码局——比尤罗·斯泽夫罗密码分析局。如果说需要是创造之母,那么或许患难就是密码破译之父。1919 - 1920 年的苏波战争中,破译苏联密码的胜利就是比尤罗·斯泽夫罗密码破译局的成功例子之一。仅在 1920 年 8 月,那时苏军已经兵临华沙,比尤罗密码局人员仍破译了 400 条敌人的讯息。直到 1926 年遇到恩格玛密码前,他们对德军通讯的监控也同样有效。

主管监听德国通讯的是上尉马克斯米廉·辛兹奇,一个忠诚的爱国者,他生长于索莫托里镇,波兰爱国主义的中心。辛兹奇曾有机会接触到商用恩格玛密码机,了解了谢尔比斯发明的所有基本原理。但不幸的是,商用机与军用机在每一个扰频器内的配线都不尽相同。如果不知道军用密码机内部配线的正确位置,辛兹奇就没有机会破译由德军发送的信息。他对破译恩格玛密码感到非常沮丧,某一段时间内甚至雇佣了一个自称有透视能力的人,从截获的德军密码信息中,疯狂地尝试祷告祈求,寻找破译的契机。毫不奇怪,透视者不可能给比尤罗·斯泽夫罗人带来他们所需的突破。这样,破译恩格玛密码的第一步工作就留给德国的一个背叛者,汉斯·西罗·施米特来完成。

汉斯·西罗·施米特,1888 年生于柏林,是家中的第二个儿子,父亲是杰出教授,母亲是贵族。第一次世界大战时,施米特在德国军队中作为一名军官,前途无量;但战后依据凡尔赛公约德军实行裁员,他被认为没有价值而不能留在军队中。不久,他尝试作一名商人,但战后萧条和通货膨胀迫使他的肥皂厂关闭,他和他的家庭也濒临破产的边缘。施米特一系列失败的耻辱感更由于他的兄长鲁道夫的成功而逐渐加深。鲁道夫也参加了第一次世界大战,战后被留在军队中。在 20 世纪 20 年代的 10 年中,鲁道夫官运亨

通，最后提升到德国陆军通信参谋部的首席长官。他负责保证德国陆军通讯的安全，而实际上就是鲁道夫正式批准了在军队中使用恩格玛密码机。

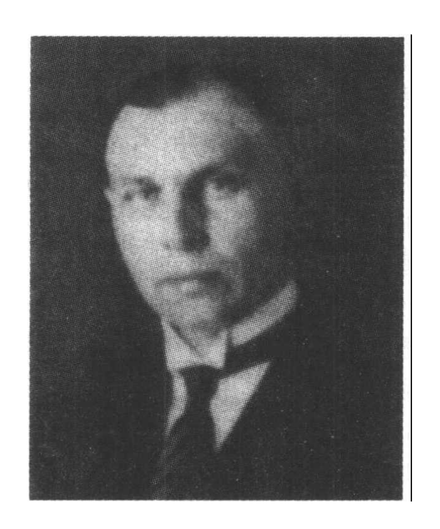


图 41：汉斯·西罗·施米特

在施米特的生意失败后，他被迫向哥哥请求帮助。鲁道夫在柏林的切夫瑞尔斯为他安排了一个工作，负责管理德国人通讯的加密。这里是恩格玛密码的指挥中心，高度机密军事机构，专门处理非常敏感的信息。当汉斯·西罗开始他的新工作时，他把他的家庭留在了巴伐利亚，在那里生活花费相对低廉。他自己独自住在昂贵的柏林，贫穷而且孤独，并忌妒他那幸运的哥哥，憎恨这个无情抛弃他的国家。其结果不可避免：将机密的恩格玛信息出卖给国外，汉斯·西罗·施米特不但可以赚得所需的金钱，而且可以通过损害他的祖国的安全，破坏他兄长的严密的机构，实现他的报复。

1931 年 9 月 8 日，施米特到达比利时韦尔维耶的豪华酒店，

与法国一个代号为"雷克思"的秘密间谍联络。以10000马克(相当于现在的20,000马克)作为交换,施米特允许雷克思对两份文件进行拍照。这些文件本来是恩格玛密码机的使用说明,尽管没有每一个扰频器内配线的详细描述,但仍然包含如何推导这些配线的信息。

正是由于施米特的背叛,盟军终于可能精确地创造德军恩格玛密码机的复制品了。但是,这还不足以让盟军密码破译员破译出由恩格玛密码机加密出的信息。这种密码保密的强度不在于密码机构造的保密,而在于这种密码机最初设置(密钥)的保密程度。如果一个密码破译员试图解码一段截获的信息,他除了需要复制一台恩格玛密码机外,仍然需要从成百上万种可能的密钥中寻找最初加密这段信息的密钥。当时的一份德国备忘录曾这样评价这种密码保密技术:"检测该密码系统的安全性表明:敌人在这种机器前将束手无策。"

明显地法国情报机关已尽到了它的责任,他们在施米特身边安排了一名情报人员,并且获得了那些表明军用恩格玛机的配线状况的文件。与此相比,法国密码破译员的工作就显得不充分,他们似乎不愿意也不能够充分利用这些新获得的信息。在第一次世界大战后,法国的密码破译员们过分自信,并且缺乏动力。他们甚至不愿意尝试建造一台德军用的恩格玛密码机,因为他们确信到了第二步(寻找密钥),找到解码某一恩格玛加密信息所需的密钥,是根本不可能的。

在获得这些文件的10年前,法国曾与波兰签署过一份军事合作协议。既然波兰人已经对与恩格玛密码有关的一切都表示了兴趣,那么,与10年前的旧协议精神相一致,法国人就简单地将施米特文件的相片交给了他们的盟友,把这个毫无希望破解恩格玛密码的任务留给了比尤罗·斯泽夫罗。比尤罗密码局认识到这些文件仅仅是破解的开始,但不像法国人,波兰人始终为再次遭受侵略

的恐惧所激励。波兰人相信一定有一条可以找到任意一项恩格玛密码机加密信息的密钥的捷径；他们还确信如果他们聪慧灵敏加上不懈努力，他们可以发现这条捷径。

除了反映扰频器内部的配线排列状况，施米特文件也详细解释了德国人如何规划所使用的密码本。在每一月中，恩格玛密码操作员都会接到一本新的密码簿，指定这一月的每一天的密钥。举个例子，在某一月的第一天，密码簿可能会指定如下日密钥：

(1)线路连接板设置：A/L - P/R - T/D - B/W - K/F - O/Y.

(2)扰频器排列：2 - 3 - 1.

(3)扰频器定位：Q - C - W.

在这里，扰频器的排列和定位可一起被看作扰频器的设置。为了执行上述的日密钥，恩格玛密码的操作员一定会按一下设置他的密码机：

(1)线路连接板设置：交换字母 A 和 L 可经由线路连接板上的一根导线连接它们，相似的方法交换 P 和 R，然后是 T 和 D，接着是 B 和 W，接着是 K 和 F，最后是 O 和 Y。

(2)扰频器排列：将扰频器 2 放入机器的狭槽 1，与此类似，扰频器 3 放入狭槽 2，扰乱器 2 放在狭槽 3。

(3)扰频器定位：每一扰频器的外缘都铭刻有字母表，这种安排允许恩格玛密码的操作员在排列扰频器时把扰频器安置于某一特定方向。在这个例子中，操作员将旋转狭槽 1 的扰频器使字母 Q 向上；旋转狭槽 2 的扰频器使字母 C 向上；旋转狭槽 3 的扰频器使字母 W 向上。

通信密码化的一种方法是按照这一天的密钥将这一天的所有通信信息都在发报前密码化。这就意味着在这整整一天中，在每段信息开始密码化前，所有的恩格玛密码的操作员都必须按照当天的密钥设定他的机器。然后，每当一份信息需要被发送时，这段信息首先需要被键入到恩格玛密码机；然后，从恩格玛密码机输出

的密码将被记录下来,交给无线电通信员来播发。在通信的另一端,无线电接收装置将记录到这段信息的密码,这段密码会被传给恩格玛密码机的操作员,由其在密钥设定相同的恩格玛密码机上输入或输出未被密码化的原信息。

这一通信过程是相当安全的,但是,重复使用同一日密钥来把一天中发送的数百条信息译成密码,将有可能变得不安全。一般而言,如果数量巨大的信息是用同一密码钥来译成密码的,对一个密码破译员来说,将这个密钥推导出来会变得相对容易。信息数量巨大的一致密码化会提供给密码破译员相应的充足的机会来确定密钥。举个例子,回到前文所谈到的简单的单字母替换密码,如果这里有几页可被分析的密文,通过重复分析密码,破译单字母替换的密码将会变得相对容易;而如果只有一两个句子供分析,破译将会很困难。

为预防上述可能情况的发生,德国人采取了很聪明的一步防范措施,即使用日密钥设定为每一条信息传递新的信息密钥。信息密钥与日密钥有相同的线路连接板设置和扰频器排列,但它的扰频器定位不同。新的扰频器定位是不被包含在密码中的,所以发送者不得不根据以下的步骤来传递给接收者。首先,发送信息者根据这一天协议的日密钥设定他的机器,包括扰频器定位,如:QCW。第二步,他随机选取一新的扰频器定位作为信息密钥,如:PGH。然后,他按照日密钥把 PGH 译成密码。信息密钥会被键人恩格玛密码机两次,仅为接收信息者提供两次核对。举个例子,发送者可能会将信息密钥 PGHPGH 译成 KIVBJE。注意,在这里两个 PGH 被译成不同的密码(前面的是 KIV,后面的是 BJE),这是因为恩格玛密码机的扰频器在每个字母译完后都会旋转,进而改变加密的全部模式。第三步,发送信息者在这时将他的机器设置改至 PGH,按照信息密钥为所要发送的加密信息。在接收者这端,机器最初将按照日密钥 QCW 设置。接收到信息的起始是六

个字母 KIVBJE，将它输入密码机后，将得出 PGHPGH。这时，接收者就会了解信息密钥为 PGH，并把扰频器设置成相应的字母，随后该机可解码信息的主体部分。

信息的发送者和接收者首先协议一个相同的主密钥。然后，不是应用这个密钥加密所有发送的信息，而是使用这个密钥为每条信息的新密钥加密，此后再使用这新密钥为相应的信息加密。假如德国人没有使用信息密钥，那么所有的通讯即可能包含着数百万字母的数万条信息，也即将按照同一个日密钥加密。但是，如果日密钥仅仅加密信息密钥，那它所加密的原文数量将极有限。例如每天中有 1000 条信息密钥被发送，日密钥所加密的字母则仅为 6000 个。另一方面，因为每条信息密钥是随机选取的，且仅被用来只加密一条信息，这条信息密钥所加密的是有限的原文，可能只有几百个字母。

据表面所见，这个系统似乎是不可能攻破的，但波兰密码破译员并没有被表面吓倒。他们准备探索每一条途径来找出恩格玛密码机及它交替使用日密钥和信息密钥方法的弱点。在对抗恩格玛密码机的斗争中站在最前面的则是全新的一类密码破译员。几个世纪以来，那些语言结构方面的专家一直被认为是最好的密码破译员，但是，恩格玛密码机的出现促使波兰人改变他们招募新密码破译员的策略。恩格玛密码是一种机器密码，由此比尤罗密码局推论：一个更科学化的头脑对破译恩格玛密码可能会更有帮助。比尤罗局组织了一个密码学课程，并邀请了 20 位数学系学生来参加，每一个学生都要求发誓保密。所有这些数学系的学生都是来自 Poznan(波兰语)的大学。尽管这所大学不是波兰最著名的科研机构，但它坐落在这个国家的西部，这一地区在 1918 年前还属于德国，所以这些数学系的学生都精通德语。

20 人中有三位表现了破译密码的才能，并因此被比尤罗密码局招募。在他们中最有天赋的是玛丽安·雷白斯基，一个害羞，带

着眼镜的23岁年轻人。在此之前,他为了在保险业获得一个职位而学习概率。尽管他在大学中只是一个刚合格的学生,但在比尤罗密码局他找到了理想的职业。在面对更富挑战性的恩格玛密码前的学习期间,雷白斯基破解了一系列难度很大的传统密码。此后,他完全单独工作,集中他所有的精力在恩格玛机的复杂结构上。作为数学家,他会尽量分析机器操作的各个方面,探索扰频器和线路连接板的连线的作用。但是,当与其他的数学家一起工作时,他的工作除需要逻辑外还更需要灵感。就像战时的另一位数学密码破译家所说的那样,一个有创造力的密码破译员为了完成智力上的成就,必须时刻都保持饱满的精神状态。

雷白斯基攻击恩格玛密码的策略集中在敌人通讯保密是建立在重复之上这一事实:重复导致模式,而模式促进密码破译。在恩格玛密码中最明显的重复是信息密钥,它在每条信息的起始部分重复两次。如果操作者选择ULJ作为信息密钥,他就会将其连续译成密码两次,这样ULJULJ译成密码后为PEFNWZ,操作者将在实际的信息前发送这段密码。德国人为避免由无线电干扰和操作者失误造成的错误,要求每条信息密钥被重复两次,但他们并没有预见到这样会危害到通讯的安全性。

每天,雷白斯基都会发现他又有一批新截获的信息。所有的信息都是以六字母开始的,这六个字母是三字母信息密钥按照预先协议的日密钥重复两次译成密码获得的。举个例子,他可能截获到四条以下面信息密钥起始的信息:

	1st	2nd	3rd	4th	5th	6th
信息 1	L	O	K	R	G	M
信息 2	M	V	T	X	Z	E
信息 3	J	K	T	M	P	E
信息 4	D	V	Y	P	Z	X

在每一行中,字母 1 和字母 4 都是相同字母的密码输出,即信息密钥的第一个字母。同样,字母 2 和字母 5 也是同一个字母的密码输出,即信息密钥的第二个字母。字母 3 和字母 6 也是同一字母的密码输出,即信息密钥的最后一个字母。举个例子,在信息 1 中,L 和 R 是同一字母的密码输出,该字母是这一信息密钥的第一个字母。相同字母译成密码不同的原因——就如第一字母先被译成 L,然后是 R——是因为在两次加密过程中,恩格玛机的扰频器 1 旋转 3 步,彻底改变了对照的模式。

L 和 R 是同一字母的加密密码这一点,使得雷白斯基能够推导恩格玛机的初始设置,并作出细微限制。初始扰频器的设置,我们并不知道;为信息密钥的第一个字母加密,这个字母我们也不知道;译成密码 L,然后,是从初始设置旋转三步后得到的另一模式的扰频器设置,这我们仍旧不知道;将信息密钥的同一字母译成密码,就得到 R。

这些推导得到的限制看上去含糊不清,充满了种种未知,但是至少它证明字母 L 和 R 最初是与恩格玛密码机的初始设置——日密钥相关。当每有一份新的信息被截获,确定信息密钥重复的密码字母 1 和 4 的其他关系是可能的。所有这些关系都是恩格玛机的初始设置的反映。举个例子,在上面举的例子中,第二条信息可告诉我们 M 和 X 是相关的,第三条信息告诉我们 J 和 M 是相关的,第四条信息告诉我们 D 和 P 是相关的。雷白斯基通过将这些关系制表开始概括字母的相关性。就目前我们所有的四条信

息，图表可以反映(L，R)、(M，X)、(J，M)和(D，P)之间的关系：

字母1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
字母4				P						M		R	X													

如果雷臼斯基在一天中有可能获得足够的信息，那么他就可以完成字母表相对应的所有关系。下面的表格显示字母间的完整关系：

字母1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
字母4	F	Q	H	P	L	W	O	G	B	M	V	R	X	U	Y	C	Z	I	T	N	J	E	A	S	D	K



图 42：玛丽安·雷臼斯基

雷臼斯基不知道日密钥的情形，也不知道是何种信息密钥被选用，但他确实知道正是日密钥与信息密钥导致了表中的关系。

如果日密钥不同,字母关系表会完全不相同。下一个问题是是否存在这样的一种方法即通过对关系表的观察就可确定日密钥。雷臼斯基开始在关系表中寻找可以预示日密钥的模式和构造,最后,他开始研究一类独特的模式,这类模式的特点是与一系列字母相关。举个例子,在关系表中,第一行的字母 A 与末行的字母 F 相关,所以,下一次雷臼斯基会在首行查找字母 F。在表中证实字母 F 是与末行的 W 相关的,他就会再回到首行查找字母 W。这回,证实首行的字母 W 是与末行的字母 A 相关的,而 A 正是我们开始时的字母,这样,一个字母链就完成了。

通过对字母表中剩余字母的查找,雷臼斯基可以建立更多的字母链。他把所有的字母链列于纸上,并注明每个字母链相关链环的数目:

A→F→W→A 3 链环

B→Q→Z→K→V→E→L→R→I→B 9 链环

C→H→G→O→Y→D→P→C 7 链环

J→M→X→Z→T→N→U→J 7 链环

目前我们已经考虑了六字母重复密钥的第一字母和第四字母之间的联系。事实上,雷臼斯基会重复我们前面的全部步骤,推出字母 2 和字母 5,字母 3 和字母 6 的所有关系,并确定每种关系下的所有字母链和相应字母链的链环数。

雷臼斯基注意到字母串每天都在改变。有时出现许多短的字母链,有时是比较长的字母链。当然,在字母链中的字母每一天都在改变。字母链这些特征显然是由于日密钥设定的改变造成的——是线路连接板设置和扰频器排列,扰频器定位共同作用的复杂结果。但是,剩余的问题是雷臼斯基怎样才能从这些字符连接中确定日密钥。在 10^{16} 种可能的日密钥中究竟是哪一条密钥是与

特定模式的密码链条相关,可能性实在是过于巨大了。

在这一点上,雷白斯基表现了不同寻常的洞察力。尽管线路连接板设置与扰频器设置都对密码链的具体细节有影响,但它们对链条的影响在某种程度上是可以被区分的。特别是链条的某一特性完全依赖于扰频器的设置,并与线路连接板设置是完全无关的:字母链条链环的数目纯粹是扰频器设置的结果。举个例子,让我们继续上面的例子,假定日密钥的线路连接板设置中是将 S 与 G 互换。如果我们打算改变日密钥设置的某一要素,把 S 与 G 之间的导线移除,再用导线交换,比方说,T 和 K 来代替,然后密码链条就会如下改变:

A→F→W→A 3 链环
B→Q→Z→K→V→E→L→R→I→B 9 链环
C→H→S→O→Y→D→P→C 7 链环
J→M→X→S→T→N→U→J 7 链环

字母链条中的某些字母改变了,但是,至关重要的是,每一链条的链环数目保持不变。

雷白斯基已经证明,字母链条的链环数目是扰频器设置的单独反映。

扰频器设置出现可能情形的总数是,扰频器排列的可能数 6,与扰频器定位可能的总数 17576 的乘积,即为 105456。这样,不用担心从在 10^{16}种可能中确定与特定密码链条相应的日密钥的问题,雷白斯基可以全神贯注于一个相对简单的问题:如何根据链条的链环数在 104456 种可能的扰频器设置中确定相应的一种。扰频器设置可能的数目仍然很大,但是它已经比日密钥可能的总数减小了 1000 亿倍。简而言之,破译恩格玛密码的任务已经简单了 1000 亿倍,已经落在人类可以处理的范围内。

雷白斯基继续进行他的工作。这里应该感谢汉斯·西罗·施密特的间谍活动，使雷白斯基可以有机会复制恩格玛机。他的小组开始进行繁重的琐碎工作：检查 105456 种可能的扰乱器设置，并归类每种设置产生的链条长度。完成分类工作花去整整一年的时间，但是一旦比尤罗密码局积累了这些数据，雷白斯基终于可以开始破译恩格玛密码了。

每天，他总会检查加密的信息密钥，即截获的每条信息的前六个字母，然后使用这些信息建立他的字母关系表。这将允许他追踪密码链，并建立每条链的链环数目表。例如，分析字母 1 和字母 4 会得到链环分别为 3,9,7 和 7 的四条字母链。分析字母 2 和字母 5 也会得到链环分别为 2,3,9 和 12 四条链条。分析字母 3 和字母 6 会得到链环分别为 5,5,5,3 和 8 的五条字母链。即使这样，雷白斯基仍然无法知道日密钥，但他知道所寻找的日密钥会导致三组字母链，在每组字母链中如以下数目的链条和链环：

链环数目 3,9,7 和 7，四条字母链，由字母 1 和 4 推得。
链环数目 2,3,9 和 12，四条字母链，由字母 2 和 5 推得。
链环数目 5,5,5,3 和 8，五条字母链，由字母 3 和 6 推得。

现在雷白斯基可以到他的分类目录中去寻找相应的扰频器设置了，这个目录，根据每种扰乱器设置产生的字母链类型为所有的扰频器设置做索引。雷白斯基一旦寻找到含有正确数目的字母链和链条中恰当数目链环的目录条目，就能立刻知道这一特定日密钥的扰频器设置。这些字母链是有效的“指纹”，是泄露初始扰频器排列和扰频器定位的证据。雷白斯基就像一位侦探，在作案现场寻找指纹，然后利用资料库来确定与之相配的嫌疑犯。

尽管雷白斯基已经可以确定日密钥的扰频器部分，他仍然不得不确定线路连接板的设置。虽然对线路连接板的设置来说有

1000 亿种可能，但确定线路连接板设置还是相对简单的工作。开始时，雷白斯基会先根据新建立的日密钥的扰频器部分设定他的恩格玛机复制品。然后，他会移去线路连接板上的所有导线，这样，线路连接板对加密过程就没有作用。最后，他会将一段截获的密文输入复制的恩格玛机。这样做的结果是机器中会输出几乎不可辨认的乱语，这是因为线路连接板的设置是未知的。但是，会经常有模糊可辨的短语或片断出现，例如，alliveinbelin，推测起来，这段句子可能为"arrive in Berlin"(到达柏林)。如果假设是正确的，那么就可以推断字母 R 和 L 是被互换的，并被线路连接板导线相连，而 A，I，V，E，B 和 N 则没有。通过分析其他的短语，确定其他五个被线路连接板互换的字母是完全有可能的。这样，在发现扰频器设置和确定线路连接板设置后，雷白斯基已经有了完整的日密钥，可以解码这一天所截获的任何信息。

雷白斯基通过把问题分解为确定扰频器设置和推断线路连接板两种，从而大大简化了寻找日密钥的任务。对每个问题来说，其本身都是可以解决的。最初，我们评估对所有恩格玛密钥进行检查所花费的时间将会比宇宙年龄还长。但是，雷白斯基花费了仅仅一年的时间就完成了对密码链长度的分类，而且，从此以后，他就可以在当天就找到那天的密钥。一旦拥有日密钥，他就可以与德国人拥有相同的信息，并尽可能早的破译信息。

在雷白斯基破解恩格玛密码后，德国人的通讯变得几乎透明。虽然波兰与德国并没有处于战争状态，但是波兰始终都处于被侵略的威胁中，攻克恩格玛密码无疑减轻了波兰恐惧的心情。假如说波兰人能发觉德国将军在心里是准备怎样对付波兰的，那么他们无疑将有极大的机会保卫自己。波兰国家的命运与雷白斯基息息相关，而雷白斯基并没有让他的国家失望。雷白斯基对恩格玛密码的攻克是密码破译员真正伟大的成就。我不得不在几页中概括他的工作，因此就省略了许多技术细节和解决问题时所遇到的

死胡同。恩格玛机是一种复杂的密码机,破译它的密码需要巨大的智力力量。我希望我的简单叙述并没有误导你,使你低估雷白斯基的卓越成就。

波兰人成功破译恩格玛密码应该归功于三点:恐惧、数学和间谍。如果没有对侵略的恐惧,开始时波兰人就可能被恩格玛密码表面上的不可攻克吓退。而如果没有数学,雷白斯基根本就不可能分析字母链。如果不是秘密代号"阿斯克"的施米特和他的文件,扰频器的配线结构根本就不可能知道,密码破译工作也不可能开始。赞扬施密特对破译密码的贡献,雷白斯基一点也不犹豫:"'阿斯克'的文件就像天赐甘露,所有的门一下子就都打开了。"

多年来,波兰人成功地使用雷白斯基的技术来监听德国人的通讯。当赫尔曼·戈林在 1934 年拜访华沙时,他完全不知道他发回国内的通讯都被截获并被解译。当他和其他德国要人在离比尤罗·斯泽夫罗办公室不远的无名战士墓敬献花圈时,雷白斯基从他的窗户向下望着他,他为能够读到德国人的绝大部分秘密通讯而满足。

即使当德国人对他们传送信息的方法作了微小的改动,雷白斯基仍然很妥善地坚持下来。他的旧密码链长度的目录变得没有用处,但是,他没有制作新的密码链长度目录,而是设计了他的目录系统的翻译机器,这台机器可以自动搜寻正确的扰频器设置。雷白斯基的发明是对恩格玛机的一种适应,每次可快速查询 17576 种设置,直到找到相应的扰频器设置。因为有六种可能的扰频器排列,六台雷白斯基机器平行工作就变得很必要,每一台机器代表一种可能的扰频器排列。六台机器一起构成了一个工作单位,大约 1 米高,需要大约 2 小时可找到日密钥。这种工作单位被称为"炸弹",这个名字大约是反映了这种机器在查找扰频器设置时发出的滴答声。另一种说法,是雷白斯基在一家咖啡厅吃"炸弹"时("炸弹"是一种半球型的冰激凌)获得制造这种机器的灵感

的。“炸弹”有效地把解码过程机器化了。这是对恩格玛机加密过程机器化的一种很自然的反应。

在20世纪30年代的大多数时候,雷白斯基和他的同事孜孜不倦地揭示恩格玛密钥。一月又一月过去了,小组不得不面对密码破译的压力和紧张,不断地修理“炸弹”机的机械故障,频繁地处理那永无尽头的截获信息。他们的生活为寻找日密钥工作所主宰,那是最重要的信息,可以揭示加密信息的主要内容。但是,波兰密码破译员所不知道的是,他们大多数的工作是不必要的。比尤罗的长官格维多·朗热少校已经获得恩格玛的日密钥,但他把它隐藏起来,塞在他的办公桌里。

朗热通过法国人,仍然可以接受到施米特传送的信息。这个间谍的报复活动,在1931年传送两份恩格玛机的操作文件后并没有结束,此后又持续了7年。他与法国的秘密接头人雷克思接触了20次,大多数情况是在与世隔绝的阿尔卑斯山上牧羊人的小屋里,在那里接头可以不受干扰。每次会面,施米特都会交给雷克思一本或几本密码簿,每本密码簿都含有一个月内的所有密钥。这些密码簿与分发给德国所有恩格玛密码操作员的完全一样,含有为信息加密和解码所需的全部信息。施米特总共提供了包含38个月的日密钥的密码簿。这些资料本来会节省雷白斯基大量的时间和精力,为直接发明“炸弹”机提供必要的捷径,并且可以节省比尤罗用在其他方面工作的大量人力。但是,这个过分狡猾的朗热决定不告诉雷白斯基这些日密钥的存在。朗热认为,不把日密钥的资料交给雷白斯基,就可以使雷白斯基为无法获得日密钥的时间做准备,而这种时候是不可避免地一定会到来。朗热知道如果战争爆发,施米特不可能继续进行秘密会面,那时雷白斯基就被迫自食其力。朗热认为雷白斯基在和平时代就应该这样准备好,就如俗语:为未来的可能做准备。

1938年12月,当德国密码译解员增加了恩格玛机的安全性

时,雷臼斯基的技术最终达到了极限。恩格玛机的操作员增加了两个新的扰频器,这样,扰频器的排列就变为从 5 个可能的扰频器中任意选取三个。过去,只有三个扰频器被用来选择(标为 1、2、3),仅有六种可能的排列方式,但是现在又有两个额外的扰频器(标为 4、5)可被选择,排列的可能升为 60 种,如表 10 所示。雷臼斯基的第一个挑战是解决两个新扰频器内部的配线结构。更让人忧虑的是,雷臼斯基还不得不新建造 10 倍于现有数量的"炸弹"机,每一台"炸弹"机都代表了一种不同的扰频器排列。而仅建造这些"炸弹"机所需的绝对费用就已经是比尤罗全年度器材预算的 15 倍。又一个月后,形势变得更加恶劣,德国人把线路连接板的导线从 6 条增加到 10 条。这样,在线路接入扰频器之前,就由原来的 12 个字母被交换增加到现在的 20 个字母被交换。密钥可能的数目也增加到 1.59×10^{20}。

表 10:5 个扰频器可能的排列

三个扰频器可能的排列	两个额外扰频器导致的额外排列								
123	124	125	134	135	142	143	145	152	153
132	154	214	215	234	235	241	243	245	251
213	253	254	314	315	324	325	341	342	345
231	351	352	354	412	413	415	421	423	425
312	431	432	435	451	452	453	512	513	514
321	521	523	524	531	532	534	541	542	543

在 1938 年,波兰人截获和破译密码达到了鼎盛时期,但是 1939 年初,新的扰频器和额外的线路连接板导线阻碍了智力的奔

流,破译密码显得不可能。雷臼斯基在过去的几年中曾大大推动了密码破译的进展,但现在也变得很迷惑。他已经证明恩格玛密码并不是不可破解的,但是现在没有所需的核对每一扰频器设置的资料,他无法找到日密钥,也根本不可能破译信息。在这种令人绝望的环境下,朗热很可能会试图把从施密特手中得到的日密钥交给雷臼斯基,但是日密钥再也不会被传送了。在新的扰频器被引入前,施密特切断了与秘密接头人雷克斯的联络。7 年来,施米特一直在提供因波兰人的发明而显得多余的日密钥资料,现在,当波兰人急需这些日密钥的资料时,这些资料却显得不可能了。

新恩格玛密码的不可攻破性无疑对波兰是毁灭性的打击,因为恩格玛密码不仅仅是通讯的一种方法,它是希特勒闪电战战术的核心。奇袭战法(闪电战)意味着快速、猛烈和联合的攻击,这意味着大军团坦克师必须与其他协同作战的部队,包括空军和步兵,保持密切联系。此外,地面部队得到空中部队(德国)斯图卡式俯冲轰炸机的支持,必须依赖前线部队和后方机场之间的有效和安全的通讯。人们评价闪电战战术"袭击的速度是通过通讯的速度完成的",如果波兰人无法破译恩格玛密码,他们就没有希望阻挡德国人的攻击,而德国人的侵略很明显就会在几个月内进行。德国已经占领了苏台德区(在捷克斯洛伐克西北部),并且在 1939 年 4 月 27 日废除了对波兰的不侵略条约。希特勒反波兰的花言巧语已经变得愈来愈恶毒。朗热下定决心如果波兰被侵略,那么它密码破译上的突破决不能丢失——这一成就一直对其他盟军保密。如果波兰不能因雷臼斯基的工作来得到好处,那么至少盟军应该有机会利用和发展它。法国与英国,可能会有额外的资源,可以有充分利用"炸弹"机的构想。

6 月 30 日,朗热少校致电法国和英国与他同样职位的盟友,邀请他们到华沙来讨论有关恩格玛密码的紧急事宜。7 月 24 日,法国和英国的高机密码破译员抵达了比尤罗的司令部,他们一点

不知道将会面对什么。朗热引领他们进入一间房间，房间中摆放着一个覆盖着黑布的物体。他揭开黑布，戏剧式地将一台雷日斯基的“炸弹”机展示给他的盟军同僚。当他们听说雷日斯基几年前就已经破译恩格玛密码时，非常震惊。波兰在破译密码方面领先世界其他国家 20 年。法国人尤为惊讶，因为波兰人的工作正是基于法国谍报工作的结果。法国人之所以把施米特的信息交给波兰人，是因为他们确信这些信息是无用的，但波兰人证明他们错了。

作为最后的惊喜，朗热提供给法国人和英国人两台恩格玛机的复制品和“炸弹”机的蓝图，这些都将通过外交途径海运到巴黎，从那里，在 8 月 16 日，其中一台恩格玛机将送往伦敦。这台机器会作为作家萨夏·吉特里和他的演员妻子伊冯娜的行李的一部分秘密进入伦敦，这是为了不引起监视港口和机场的德国间谍的怀疑。两个星期后，在 9 月 1 日，希特勒入侵波兰，战争爆发了。

从不咯咯叫的鹅

13 年来，英国和法国都认为恩格玛密码是无法破解的，但是现在又有了希望。波兰人的发现表明恩格玛密码存在缺陷，这极大鼓舞了盟军密码破译师的志气。波兰人破译恩格玛密码的进展因引入新的扰频器和额外的线路连接板导线而受阻，但是恩格玛密码再也不被认为是完美无缺的密码。

波兰人的突破也向盟军表明了雇用数学家作为密码破解员也是件必要的事。在英国，40 号房里面大多数都是语言学家和古典学者，但是现在 40 号房正在努力召集数学家和科学家，希望能平衡这个工作小组。40 号房的人开始与各自在牛津和剑桥大学时的同学广泛联系，召集数学科学家。他们也通过女校友网络吸收从纽汉大学、格顿大学以及剑桥大学毕业的女同胞们。



图 43:海因茨·古德里安将军的命令传送器。在左下角可见到一个正在使用的密码机。

新招来的人员并没有被带到伦敦的40号房，相反他们来到了位于白金汉郡的布莱切里庄园，这里是政府密码学校（GC&CS）所在地，密码学校是个新成立的密码破解机构，由40号房管理。这里能容纳更多的人，这一点很重要，因为战争一旦爆发将会截获大量的加密信息。在一战期间，德国每月内交传送的信息达200万单词，因而可以预见，二战期间，由于无线电的广泛使用，德国的信息传送量将达到每天200万单词。



图44：1939年8月，不列颠的高级密码破译家来到了布莱切里庄园以评估它是否合适于做新的政府密码和密码学校。他们为避免引起地方居民的怀疑，声称自己为莱德利上尉的射击队。

在布莱切里庄园中心是一座维多利亚时代都铎－歌德式豪宅，由19世纪金融家赫伯特·利昂兴建。这座豪宅有图书馆、餐厅以及华丽的舞厅，这里是整个布莱切里组织的管理中心。司令官阿拉斯泰尔·丹尼斯顿是政府密码学校的总管，在豪宅的底层有

一间办公室,面向整个庄园。从这里看去,你的视野内充满了无数的小屋。在这些临时搭建的木屋里进行着各种不同的密码破解活动。例如,6 号屋主要负责截获德国陆军的通讯,再将截获的电文交到 3 号屋。3 号屋的情报人员负责译出信息。8 号屋则将精力集中在德国海军的通讯上,将截获的电文交给 4 号屋,4 号屋再进行破译和收集情报。刚开始的时候,布莱切里庄园只有 200 名工作人员,但不到 5 年的时间,豪宅加上木屋共吸纳了近 7000 名男女。

1939 年秋天,布莱切里的科学家和数学家学习了恩格玛密码的破译系统并很快掌握了波兰人的技术。由于恩格玛密码自身的发展已使破解它的难度提高了 10 倍,但是布莱切里比波兰的比尤罗·斯泽夫罗拥有更多的员工和资源,因而还能应付得了。每天 24 个小时,英国的密码破解员都做着重复的事情。午夜时分,德国恩格玛操作员将更换一个新的日密钥,这时,无论布莱切里在前一天取得什么突破都不能再被用来解密信息了。密码破解者不得不重新开始一天的工作来确定新的日密钥。这可能需要几个小时,但是一旦他们发现了当天的恩格玛设置,布莱切里小组就开始破译他们收集到的德军信息,即可得到对战事有价值的情报。

对于一个司令官来说出奇制胜是战场上一个重要的法宝。但是如果布莱切里破解了恩格玛,那么德国的计划将显示得一清二楚,英国就能够掌握德国最高司令官的思想。如果英国人得知德军将发动快速攻击,那么他们会马上调遣援军或者采取回避措施。如果英国人能够破译德国对自身弱点的讨论,那么盟军的进攻就有了针对性。布莱切里的解密工作具有极高的重要性。例如 1940 年 4 月当德军进攻丹麦和挪威时,布莱切里提供了一份关于德军行动的详细的计划书。同样在对英国的战役中,密码破译师提前警告英军,德军将进行轰炸,包括轰炸的时间和地点。他们也能够给出德国空军编队的动向,损失的飞机数以及更换的速度。

布莱切里将所有的信息都发给军情 6 处，再由军情 6 处传到海、陆、空三军战场上。



图 45：布莱切里的密码分析师在打圆场棒球

在影响战争发展方向的同时，密码破译师们也会偶尔找些时间休息一下。在安全系统工作的马尔科姆·马格里奇曾访问过布莱切里，他说圆场棒球是在布莱切里工作的人们最喜爱的休闲活动；一旦布莱切里密码破译师掌握了波兰的技术，他们就开始自己寻找确定恩格玛密钥的快捷途径。例如，他们发现德国恩格玛操作员经常会选择一些意义明显的信息密钥。对每个信息，操作员应该选择一个不同的信息密钥即随机的三字母组合。然而在战场的中心，过度工作的操作员往往不会浪费精力去想每一个随机密钥，他们通常会从键盘上（图 46）输入三个相邻的字母作为一个信息密钥，例如 QWE 或 BNM。



图 46:恩格玛机键盘的布局

这些可预测的信息密钥被称作色利斯(cillies),另一种色利斯是同一个密钥被重复使用,或许就是某个操作员女友姓名的首字母,这种情况是存在的,例如 C.I.L。在破解一个恩格玛之前,密码破译师已经习惯先尝试一下各种色利斯,他们的直觉往往就是对的。色利斯不是恩格玛机器本身的弱点,而是在使用的时候暴露出人为的弱点。可见一定程度上的人为错误也会使恩格玛机器的安全性打些折扣。这种例子还有。负责编辑密码簿的人不得不决定每天该使用哪个扰频器以及每个扰频器的状态。他们一般避免每个扰频器连续两天处于同一位置,以确保扰频器的设置不可预测。因此如果我们给扰频器标号 1,2,3,4,5,那么第一天排列可能是 134,第二天则可能是 215,当然不会是 214,因为标号 4 的扰频器不允许在两天内处于同一位置。这种策略看上去似乎有点作用,因为扰频器不断的改变位置,但是德军使用这个规定实际上使英国密码破译师的工作更容易些。德军避免一个扰频器连续两天处于同一位置,意味着密码簿编辑者减少了可能一半的扰频器排列工作。布莱切里密码破译师认识到了它,并充分利用了这一点。一旦他们确定了某一天的扰频器的设置,他们就能够立刻为第二天排除可能一半的扰频器排列。因此他们的工作量就减少了一半。

同样在德军里还有一个关于插件板设置的规则,插件板设置要避免交换相邻的两个字母,也就是 S 只能和除 R 和 T 以外的字母交换。他们认为如此明显的交换应当有意的去避免。但又一次这个规定的实行极大地减少了可能密钥的数量。

由于在战争期间恩格玛机仍在继续发展，因而不断地寻找新的突破途径是必要的。密码分析师们一直在追求创新，不断地提出和改进新的方法。他们的成功有一部分就是因为他们之间这种奇异的组合，在各个木屋里有数学家、科学家、语言学家、古典学家、象棋大师甚至填单词游戏迷。一个难题会在木屋之间传来传去，直到有适当的人利用他的知识去解决它，或者部分地解决后再传给他人。6 号木屋的负责人戈登·韦尔什曼曾将他的小组形容为“一群嗅觉灵敏的猎狗”。在布莱切里有许多伟大的密码破译师和许多著名的突破，如果详细地描述每个人的贡献能写出几本这样的书。但是，如果非要提及一个人的话，那他就是阿兰·图灵，他找出了恩格玛最大的一个弱点并进行毫不留情的攻击。即使在最艰难的环境下，也正是因为有图灵，才使破解恩格玛密码成为可能。

1911 年的秋天，阿兰·图灵的母亲在靠近南印度马德拉斯的一个城镇里怀孕了，这个孩子就是图灵。他的父亲尤利乌斯·图灵是一名文职官员，尤利乌斯他的妻子尹赛尔决定将他们的儿子出生在英国，于是他们来到伦敦，1912 年 6 月 23 日，小阿兰出世了。他的父亲很快就返回了印度，15 个月后他的母亲也跟着回去了。小阿兰被留给保姆和朋友照顾，直到他长大后，去了一所寄宿学校。

1926 年，图灵 14 岁的时候，成为位于多塞特的舍伯恩学校的一名学生。图灵上学的那一天正好碰上英国总罢工，但是图灵决定第一天要去上课。他独自一人从索桑普顿骑车近 100 公里来到舍伯恩，后来当地报纸都报道了这一壮举。在学校待了一年，他被认为是个害羞笨拙的小男孩，惟一擅长的就是科学问题。舍伯恩学校的目标是想将学生变成一个全面发展的人才以适应帝国发展的需要。但是图灵并没有这份野心，因此他的学校生活总的来说并不快乐。

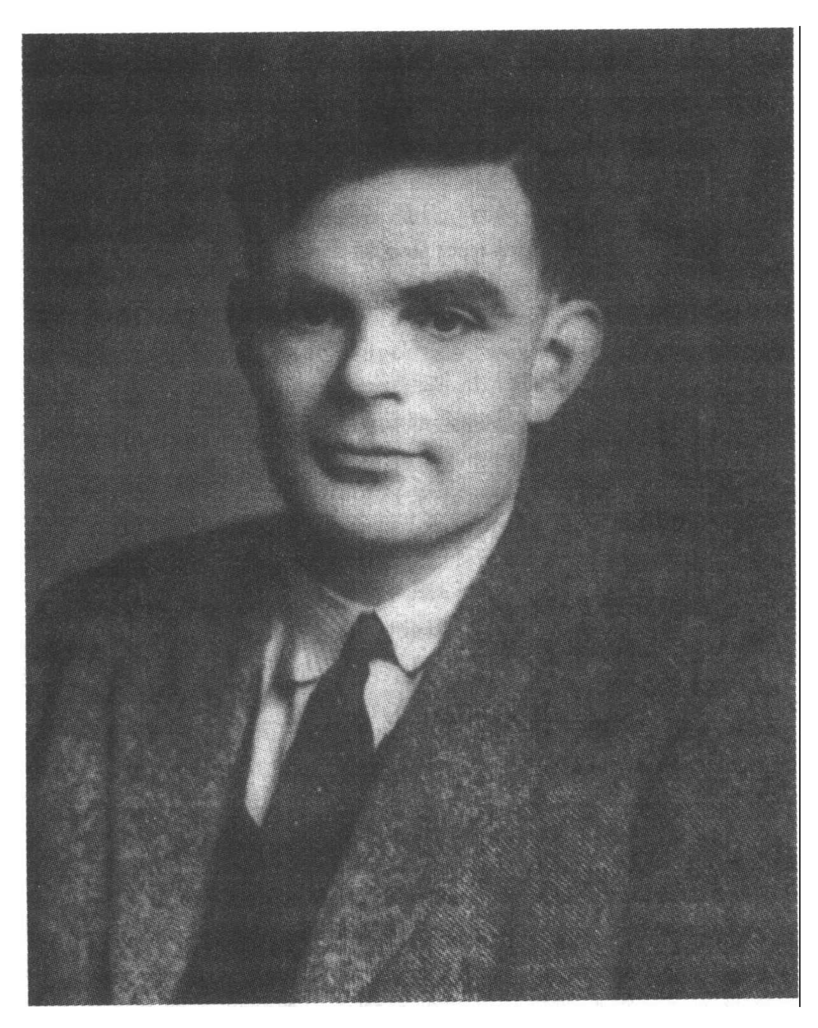


图 47:阿兰·图灵

他在舍伯恩惟一真正的朋友是克里斯托弗·马科姆,这个孩子与图灵一样也对科学有兴趣。他们经常在一起讨论最新的科学

新闻并自己动手做实验。这种关系激起了图灵对知识的好奇，但是更重要的是，这对图灵的情感也产生了深刻的影响。图灵的传记作家安德鲁·霍奇斯曾写道："这是第一次爱……有一种投降的感觉，一种执着，就像在这个黑白世界里突然出现五彩斑斓的颜色。"他们的关系持续了4年，但是马科姆似乎没有认识到图灵对他的至深感情。最终在舍伯恩的最后一年，图灵永远地失去了表白的机会。在1930年2月13日，克里斯托弗·马科姆突然死于肺结核。

图灵受到了沉重的打击，他一生中可能惟一真爱的人永远地离去了。他惟一做的就是将全部精力放在科学研究上，希望能完成他朋友的遗愿。马科姆也是极具天赋的孩子，他已经获得了剑桥大学的奖学金。所以图灵认为他也应该在剑桥赢取一席之地，这是他的义务，然后再做出一些本来属于他朋友的成果。他向马科姆的母亲要了一张他朋友的照片，当照片寄来的时候，他回信写道："我把它贴在我的桌子上，以鼓励我努力工作。"

1931年，图灵进入剑桥皇家学院。他到来的时候，那里正进行着一场激烈的关于数学和逻辑的辩论，图灵面对的是一批伟人，包括伯特兰·罗素、艾尔弗雷德·诺思·怀特海和路德维格·维特根斯坦。这场辩论的中心问题是新提出的不可判定性，这是由逻辑学家库尔特·戈德尔提出的一个有争议的论点。之前人们普遍认为理论上所有的数学问题都能够被解答。然而戈德尔表明存在一小部分传统问题的逻辑分析是无法证明的，即所谓不可判定性问题。数学家一直相信数学是一门全能的学科，但现在有人说不，他们很难接受。他们通过建立一种辨别这类尴尬问题的方法来试图挽救这门学科，这样他们就能将这些问题安全地放在一边。正是这种目的赋予图灵灵感，写出脍炙人口的数学论文《关于可计算的数字》，于1937年发表。休·怀特莫曾编了一个关于图灵生活的话剧《破解密码》，一个剧中人物询问图灵关于这篇文章的意义，图灵

这样回答:“它是关于是与非的。总的来说,它是一篇数学逻辑的技术性论文,但它也是关于困难的,是辨别是与非的困难。人们认为——大多数的人都认为,在数学中我们已经知道什么是对或错。但我们没有,远远没有。”

在寻找不可判定问题的过程中,图灵的论文还描述一种想像的机器,它能进行一些特定的数学操作或算法。换句话说,这种机器能够执行一系列事先描述好的步骤,比如将两个数相乘。图灵设想两个相乘的数字可以通过一张普通的纸输进机器里,而相乘的结果通过另一张纸输出来。图灵设想了一系列的所谓图灵机,每台机器都设计来执行一个特别的任务,例如除、平方或乘方。紧接着,图灵迈出了至关紧要的一步。

他设想了一台机器的内部工作能够被改变,并且能执行所有酝酿中的图灵机的功能。这种改变可以通过小心地插入各种需要的磁带来解决,这样根据需要就可将一台灵活的机器变成一台除法机、一台乘法机或者任何其他类型的机器。图灵称他这个假想的机器为“万能图灵机”,因为它能够解决任何逻辑上可以解决的问题。可是,解决能否回答不可判定性的问题这一点在逻辑上是不可能的,所以“万能图灵机”并不是万能的。

数学家读完了图灵的论文之后感到失望,因为戈德尔的魔鬼还没有被征服。但是也让他们安慰的是图灵给出了一个现代程序化计算机的蓝图。图灵了解巴比奇的工作,万能图灵机其实就相当于差分机2号。但是这一次图灵走得更远,他提供了一个牢固的理论基础,使计算机具有的潜能到现在都难以想像。由于当时还是1930年,还没有技术能将万能图灵变成现实。尽管图灵的理论超越了现实,但他一点也没有感到灰心丧气,他仅仅想得到数学系专家的认可,而他的论文确实被看成20世纪最重要的突破之一,毕竟图灵当时才26岁。这一段时间对图灵来说是特别的快乐和成功。在20世纪30年代图灵从一名微不足道的学生一下升为

世界精英之家国王学院的研究员。他过上了典型的剑桥教师的生活,纯数学研究加上琐事不断。1938 年,他看了一场电影名叫《白雪公主与七个小矮人》,里面有个难忘的情景是邪恶的巫婆将一个苹果泡在毒药里。后来他的同事听见图灵在不断地重复那可怕的台词:"将苹果放在毒药里蘸一下,让睡神悄悄来临。"

图灵非常珍惜他在剑桥的时光。除了学术上的成功。他发现自己处在一个相互宽恕和支持的环境中。同性恋在这个大学里是被广泛接受的,这意味着他可以自由的发展一些关系而不用担心有谁会察觉和说出来。尽管他没有严重的长期同性恋关系,但他似乎很满意自己的生活。然而在 1939 年图灵的学校生活突然被终止。政府密码学校邀请他去布莱切里成为一个密码破译师,在内维尔·张伯伦对德宣战的第二天,图灵离开了富裕的剑桥大学来到申里布鲁克安德的克罗因。

每天他骑车 5 公里从申里布鲁克安德来到布莱切里庄园,在这里他一部分时间花在木屋里参与每日例行的密码破解工作,另一部分时间则在布莱切里的智慧坛度过,这里曾是赫伯特·里昂爵士用来储藏苹果、梨子和李子的地方。当时在这里,密码破译师们经常集中分享讨论解决问题的方法,或者预测将来可能出现的问题并研究如何解决它。

图灵将注意力集中在每次德军在改变他们信息密钥交换系统的时候会发生些什么变化这一问题上。布莱切里早期的成功是依靠雷日斯基的工作,他发现了恩格玛操作员会将每个信息密钥加密两次这个事实(例如如果信息密钥是 YGB,那么操作员将加密 YGBYGB)。这种重复应该是用来防止接收员犯错,但这给恩格玛的安全性带来了一个裂缝。英国密码分析员猜测德军不久将会注意到重复密钥会降低恩格玛密码的安全性。到时恩格玛操作员将要求放弃重复密钥,这样布莱切里现在的密码破解技术将一无用处。而图灵的工作发现了另一种攻击恩格玛密码的途径,它不

依赖重复的信息密钥。

几个星期过去了，图灵了解到布莱切里积累了一个巨大的解密信息的数据库。他观察到其中有许多具有固定的结构，并仔细地研究解密信息，他相信自己有时能够预测一个没有解密的信息内容，而根据是它从何时何地发出。例如，经验表明德军每天早晨6点过后会发送一条规范的天气报告，当然是加密的。因此，在早晨6点零5分截获的加密信息几乎必然会含有单词 wetter，这是德国词语的意思是天气。军事组织通常是按照严格的规定行事，也就意味着这样的信息在格式上肯定是高度统一的。因此图灵甚至对 Wetter 这个词在密文中的出现位置都很自信。例如经验告诉他这种特别密文的前六个字母就是指明德文字母 wetter。当一篇明文和一篇密文联系起来的时候，我们称这种组合为克利巴(Crib)。图灵确信他能够利用这些克利巴来破解恩格玛密码。如果他有一个密文并且他知道其中的某一部分是什么意思，比方说 ETJWPX 代表 wetter，那么需要解决的问题就变成了如何确定恩格玛的设置，而依据就是这种设定能将 wetter 译成 ETJWPX。最实际直接的方法是让密码分析师拿一台恩格玛机，输入 wetter 看看是否得到正确的密文。如果不是，那么密码分析师就变换机器的设置，通过交换插件板连接器，重新定位或交换扰频器等，然后再输入 wetter。如果期望的密文还是没有出现，那么密码破译师再改变设置，一次又一次地改变直到发现正确的设置为止。这种方法惟一的问题是那将需要检查 1.59×10^{20} 个设置可能，因此想找到那种使 wetter 变成 ETJWPX 的设置看上去是件不可能的事。

为了简化问题，图灵尝试了雷臼斯基的方法将机器的各设置分开来考虑。他想把扰频器的设置这个问题(即哪个扰频器在插槽中以及它们各自的定位)和插件板连接器的问题分开。例如，如果他能够发现在克利巴中有些时候是和插件板连接器设置无关的话，那么他就能够切实可行地检查剩余的 1054560 种扰频器的设

置(60 种排列 × 17576 种定位)。一旦发现扰频器的设置,他就能推导出插件板连接器设置。

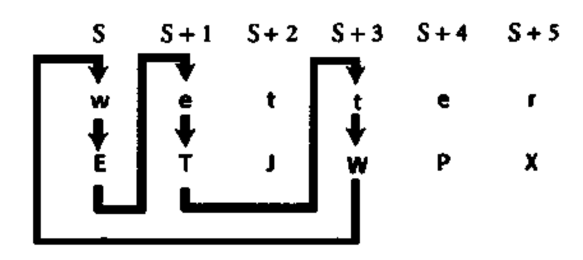


图 48:图灵的克利巴之一,显示了一个环路

最终,他的思想定位在一种特别的克利巴上,这种克利巴内部能形成一个环路,就像雷白斯基使用的链接一样。雷白斯基的链将重复的信息密钥的字母连接起来。而图灵的环路和信息密钥没有任何关系,因为他本来就认为德军会很停止发送重复的信息密钥。相反图灵的环路连接的是一个克利巴中明文和密文的字母。例如,图 48 显示的克利巴含有一个环路。记住,克利巴仅仅是猜测,但是我们假定这个克利巴是准确的,那么我们可以将字母 w→E,e→T,t→W 连接成一个环。尽管我们不知道恩格玛机器的任何设置,但我们可以用代号表示一下,我们将第一个设置标为 S。在第一个设置里,我们知道 w 被加密成 E,这次加密过后,第一个扰频器将旋转一个位置到 S+1 的设置,此时字母 e 加密成 T。混乱器再移动一个位置加密一个字母,注意这次加密的字母不在环内,因此我们忽略这个加密过程。扰频器继续向前转动一下,这一次字母又回到了环内,此时的设置是 S+3,我们知道字母 t 加密成 W。概括一下我们得到:

在设置 S,恩格玛将 w 加密成 E。

在设置 S+1,恩格玛将 s 加密成 T。
在设置 S+3,恩格玛将 t 加密成 W。

到目前为止,这个环路似乎只是一个奇怪的模式,但是图灵却坚定地认为这个环路隐含着某种关系在里面,并且为他破解恩格玛提供了所需的快捷途径。这一次图灵不是单单拿着一台恩格玛机来测试每一条设置,他开始想像有三台独立的机器,每台机器只处理环路中一个加密。第一台机器负责将 w 加密成 E,第二台负责将 e 加密成 T。第三个 t 将加密成 W。这三台机器有着完全一样的设置,区别就在于第二台机器的扰频器的定位和第一台机器的扰频器相比前进了一个位置,S+1 是它的设置标号;第三台机器的扰频器定位和第一台相比前进了 2 个位置,它的设置标号是 S+3。然后图灵想像有一个疯狂的密码分析师,他不断地变换插件板连接器,改变扰频器的排列及它们的定位,希望能最终得到准确的加密设置。但是在第一个机器中无论连接器怎么改变,其他两个机器也要跟着做同样的变换。对于扰频器的排列也是无论在第一台机器中怎么改变,其他两台机器要跟着做同样的变动。而最关键的是,对于扰频器的定位无论第一台机器里是什么状态,第二台机器都要时刻保持比第一台前进一步,第三台要比第一台前进两步。

图灵似乎并没有什么进展。密码破译师还是不得不检查1.59×10^{20}种可能的设置。而且更糟糕的是,他现在不得不同时在三台机器上检测所有的设置而不是一台。但是图灵思想的下一步却扭转了整个形势,极大的简化了过程。他想像用电线通过输入端和输出端将三台机器连接起来,如图 49 所示。这样,克利巴中的环通过电环路并行起来。图灵想像这些机器按照前所述的那样改变插件板和扰频器的设置,但只有当三台机器所有的设置正确的时候,才真正形成回路,能够允许电流通过所有三台机器。如果图

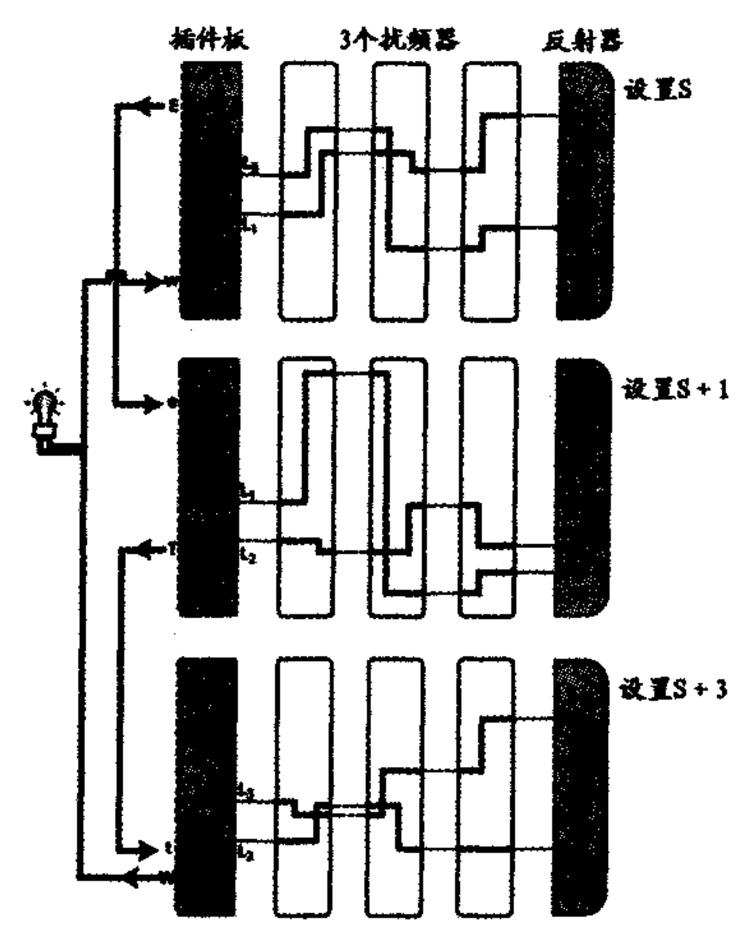


图 49:克利巴在恩格玛机中形成的环路是与电流环路平行的。三个恩格玛密码机以同样的方式装在一起。除了第二组扰频器比第一组多前进一步(记作设置 S+1)。第三组比第一组多前进两步(记作设置 S+3)。每个恩格玛机的输出端部与下一个机器的输入端相连。三组扰频器连在一起,形成一个环路,当电流走完环路后,灯炮就被点亮。这时,正确的设置就找到了。如图,环路根据正确的设置形成了。

灵在环路上放置一个灯泡，那么电流将使灯泡发光，也就是说正确的设置已经发现。此时，为了能够点亮灯泡，这三台机器仍然需要检验 1.59×10^{20}种可能的设置。但是，到目前为止所做的一切事情都是为图灵的最后一步飞跃做准备。这后一步能使整个工作容易 1×10^{15}倍。

图灵已经建立了他的电流环路，实际上这已经抵消了插件板的影响，因此能容许他忽略近上万亿种的插件板的设置。图 49 显示在第一台恩格玛里，字母 w 产生的电流通过扰乱器后形成一个我们不知道的字母，我们姑且称之为 L1。然后电流经过插件板所在的 L1 变成了 E。这个字母 E 再通过电线连到第二台恩格玛的字母 e 上。随着电流经过第二个插件板它又变回了 L1。换句话说，这两个插件板的作用彼此相互抵消了。同样在第二台恩格玛中电流继续通过扰频器后以我们不知的字母 L2 回到插件板。经过插件板后变成了 T，T 又和第三个恩格玛机上的 t 字母相连。随着电流经过第三个插件板它又变回了 L2。简言之，插件板在整个环路中相互抵消了彼此的影响，因此图灵可以完全地忽略它们。

图灵只需要将第一组扰频器的输出端 L1，直接连接到第二组扰频器的输入端，还是 L1 等。然而遗憾的是，他不知道字母 L1 究竟是什么，因此他必须将第一组扰频器的 26 个输出端和第二组扰频器相应的 26 个输入端相连，依此类推。这样就有了 26 个电流环路，每个环路都有一个灯泡来标示电流环路的接通。然后这三组扰频器只需简单地测试 17576 种可能的定位，只要注意第二组扰频器比第一组多前进一步，第三组又比一组多前进两步。最终，当正确的扰频器设置出现的时候，其中一个环路将完成前后连接，灯泡被点亮。如果扰频器每秒钟改变一种定位的话，那只需 5 个小时就能测完所有的定位。

现在只剩下两个问题。第一，这三台机器扰频器的排列可能一开始就是错误的，因为恩格玛机有 5 个扰频器供使用，但它每次

只用其中的3个。这就产生了60种可能的排列。因此如果17576种定位全部检查完后灯始终没亮,那么就必须更换这60种排列中的另外一种再做尝试,并且要不断地尝试下去,直到电流完成回路。密码破译师完全可以同时开展60组这样的测试以节省时间。

第二个问题是一旦扰频器的排列和定位被确立后,该如何确定插件板连接器的设置。这个问题相对比较简单。首先将恩格玛机的扰频器排列和定位设置正确,密码破译师只需将密文输进去观察出现的明文。如果得到的结果是tewwer而不是wetter,那么很明显应该插入一个连接器能够交换w和t。再输入一些其他的密文即可揭示其他连接器的设置。克利巴、环路和电线连接的机器这三者综合在一起最终构成了密码破译学一件不朽之作。也只有图灵,利用他独特的数学背景,能够做到这一点。他的图灵机的遐想本来是希望解决数学上深奥的不可判定性,但是,这个纯学术研究,却促使图灵在头脑中设计出实用的解决少见难题的机器。

布莱切里筹集了10万英镑要将图灵的想法变成能够工作的机械装置。由于它的机理和雷白斯基的炸弹有一定的相似性,图灵的装置仍称为"炸弹"。每个图灵"炸弹"由12组相连的恩格玛扰频器组成,因而能够处理更长的字母环。整个装置高2米,宽2米。图灵在1940年初的时候完成了他的设计,由莱奇沃斯的英国机械工厂负责加工生产。在等待"炸弹"完工的时候,图灵继续在布莱切里日夜工作。关于他突破恩格玛的消息很快就在其他高级密码破译师之间传开,他们认为图灵是极具天赋的密码破解大师。布莱切里一位密码破解者皮特·西尔顿说:"很显然阿兰·图灵是个天才,但他是个易亲近的,友好的天才。他总是愿意抽出时间和精力来解释他的思想;而且,他不是个兴趣很窄的专业人员,他的奇思异想覆盖了极广的科学领域。"

但是,在政府密码学校发生的一切事情都属于高度机密,因此

布莱切里庄园以外没有人知道图灵所取得的卓越的成就。例如他的父母甚至一点也不知道图灵是个密码破解员，更不用说是英国最著名的密码破译师了。他曾经告诉他的母亲他在做一些军事研究方面的工作，但没有详细说明。他的母亲为此感到有点失望，这份工作并没有改变她儿子衣冠不整的形象，她认为儿子至少也该理一种看得过去的头发。尽管布莱切里受军方管理，但是他们承认他们有时不得不容忍这些教授形象上的邋遢和古怪。图灵很少修面，他的指甲里充满了泥垢，他的衣服也是皱皱巴巴。关于军方是否容忍了他的同性恋行为还不为人所知。布莱切里的一位老兵杰克·古德评述道："幸运的是当局不知道图灵是个同性恋者，要不然我们可能会输掉这场战争。"

第一台"炸弹"原型命名为胜利，于 1940 年 3 月 14 日送入布莱切里。这台机器立刻就投入运行，但是最初的结果却并没有令人满意。机器比预期的要慢得多，花费了近一个星期的时间才找到某个密钥。因此大家又商议如何提高机器的效率，几个星期后就提交了一份改进设计。改造炸弹又用了 4 个多月的时间。1940 年 5 月 1 日，德国改变了他们的密钥交换规则。他们不再使用重复的信息密钥。因而破译恩格玛的成功率急剧下降。信息中断一直持续到 8 月 8 日，那时新的"炸弹"到来了，这次命名为"上帝的羔羊"，这台机器和图灵的设想一模一样。

18 个月内，先后有 15 余台"炸弹"投入工作，利用克利巴检查扰频器设置和揭示密钥，就像上百万个在编织的针一样卡嗒卡嗒地响个不停。如果一切进行顺利，那么每台机器能在 1 小时内发现恩格玛密钥。一旦根据某个信息确定了插件板连接器和扰频器的设置(即信息密钥)，那么很容易就推出日密钥。这一天发送的所有其他的信息都将被解密。

尽管"炸弹"代表了密码破译学上一个关键的突破，解密并没有成为一件公式化的事情。在"炸弹"开始寻找一个密钥之前，仍

有许多的问题需要克服。例如，要想使“炸弹”工作起来，首先需要一个克利巴。然后高级密码破译师将克利巴交给“炸弹”操作员，但是不能保证密码分析师猜对了密文的正确意思。即使他们确实有正确的克利巴，那也有可能所处的位置是错误的——密码破译师可能猜到一个加密的信息中含有特定的一个词组，但是将这个词组和密文对应时发生错误。然而有一种小技巧能够检查一个克利巴是否处在正确的位置。

在下面的克利巴中，密码破译师相信明文是正确的，但他不能肯定他是否将明文和密文正确地配对起来。

猜测的明文　　w e t t e r n u l l s e c h s
已知的密码　I P R E N L W K M J J S X C P L E J W Q

恩格玛机器的一个特点就是它不能够将一个字母加密成该字母本身，这是由于存在反射器的原因。字母 a 永远不能加密成 A，字母 b 也永远不能加密成 B 等。这样以上的克利巴配对也一定是错误的，因为 wetter 中的第一个 e 和密文中的 E 发生了配对。要找到正确的联配，我们只需简单地将密文和明文来回移动直到没有同样的字母自身配对。在以上的例子中我们将明文向右移动一个位置后就没有了不合规则的加密，那么此时克利巴可能处在正确的位置，可以被“炸弹”用来解密。

猜测的明文　　　w e t t e r n u l l s e c h s
已知的密码　I P R E N L W K M J J S X C P L E J W Q

布莱切里收集的情报只交给最高级军官和战争委员会里指定的人员。温斯顿·邱吉尔充分认识到布莱切里解密工作的重要性，在 1941 年 9 月 6 日，他慰问了密码破解者。当他见到一些密码破译师时，他感到非常的吃惊：给他提供如此有价值情报的人不仅是

数学家和语言学家，而且是一大堆稀奇古怪的人，他们形成了一个奇怪的团队，其中有瓷器专家、布拉格博物馆馆长、英国象棋冠军和许多桥牌专家。邱吉尔对身旁的国家秘密情报服务负责人斯图尔森·孟席斯小声说："我要你不惜一切努力给我办好，但我没想到你做得如此细腻。"除了这些言论，他还对那帮五花八门的队伍产生了极大的兴趣，把他们称为"会下金蛋的鹅"。

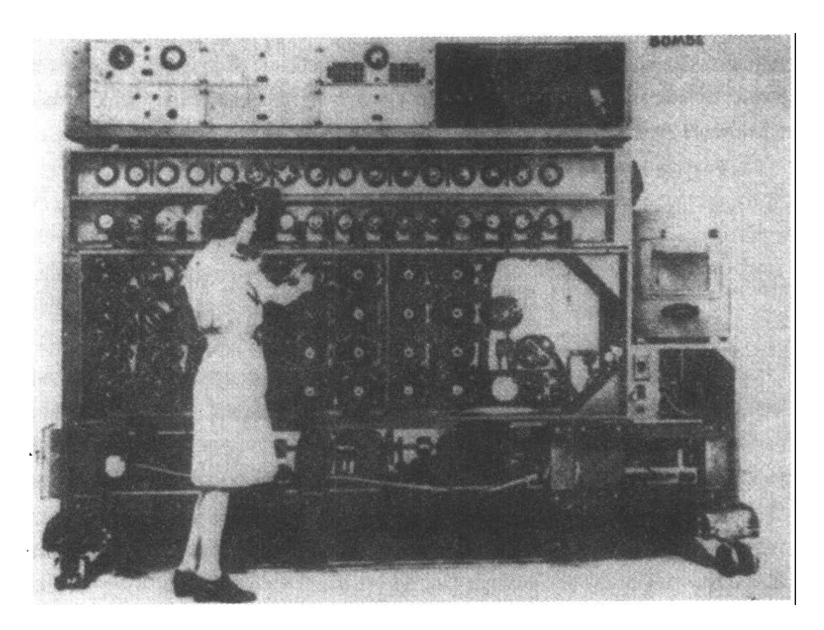


图 50:一个正在运作的"炸弹"

这次慰问是想鼓舞密码破解者的士气，向他们表明他们的工作受到了最诚挚的感谢。但这次访问也给了图灵和他的同事很大的信心，就在危机时刻他们可以直接地接近邱吉尔。为了最大限度地利用"炸弹"，图灵需要更多的工作人员，但他的要求被爱德华·特拉维斯长官拒绝了，爱德华·特拉维斯刚接管布莱切里不久，

他不认为招收更多的人是正确的。1941年10月21日，密码破译师终于有所反抗，他们直接写信给了邱吉尔：

尊敬的首相：

几个星期前您来视察过我们，我们感到很荣幸。我们相信您将我们的工作看得很重要。您应该知道由于特拉维斯长官的能力和远见，我们都配备上了足够的“炸弹”来破解德国恩格玛密码。然而，我们认为您还应该知道这项工作现在被暂时终止了，主要是因为我们没有足够的人手来操作它。我们直接写信给您的一个原因是几个月来通过正常渠道，我们已经做了一切我们能做的事情，但我们对取得的进展感到非常失望，我们觉得没有您的参预……

我们是您忠实的仆人。

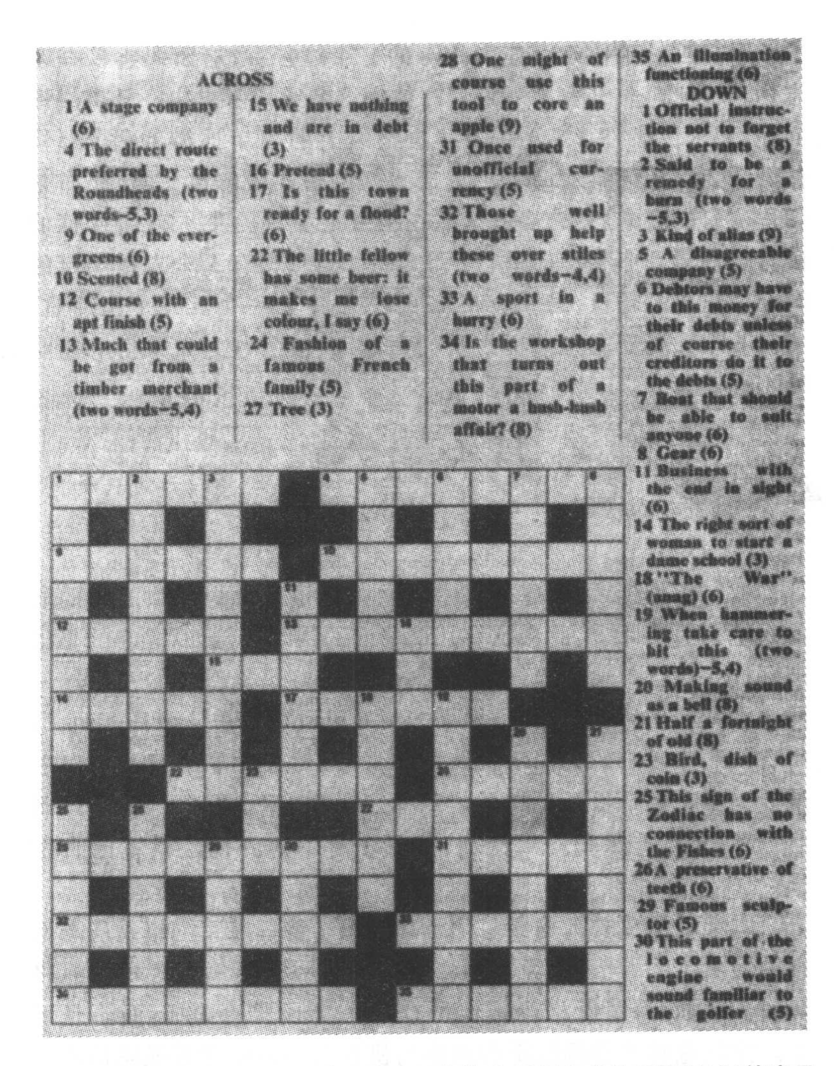
图灵(A.M.Turing)
韦尔什曼(W.G.Welchman)
亚历山大(C.H.O'D.Alexander)
米尔纳－巴里(P.S.Milner－Barry)

邱吉尔毫不犹豫地立即作出反应，他给他的人事办公室发了一个函：

今天的任务

确保他们要求的一切事情都具有绝对优先权，办完之后再向我汇报。

从此以后，在招募和所需品上再也没有任何阻碍。1942年底，共有49台“炸弹”，并且在布莱切里北面加赫斯特马诺又新建



ACROSS

1 A stage company (6)

4 The direct route preferred by the Roundheads (two words–5,3)

9 One of the evergreens (6)

10 Scented (8)

12 Course with an apt finish (5)

13 Much that could be got from a timber merchant (two words–5,4)

15 We have nothing and are in debt (3)

16 Pretend (5)

17 Is this town ready for a flood? (6)

22 The little fellow has some beer: it makes me lose colour, I say (6)

24 Fashion of a famous French family (5)

27 Tree (3)

28 One might of course use this tool to core an apple (9)

31 Once used for unofficial currency (5)

32 Those well brought up help these over stiles (two words–4,4)

33 A sport in a hurry (6)

34 Is the workshop that turns out this part of a motor a hush-hush affair? (8)

35 An illumination functioning (6)

DOWN

1 Official instruction not to forget the servants (8)

2 Said to be a remedy for a burn (two words –5,3)

3 Kind of alias (9)

5 A disagreeable company (5)

6 Debtors may have to this money for their debts unless of course their creditors do it to the debts (5)

7 Boat that should be able to suit anyone (6)

8 Gear (6)

11 Business with the end in sight (6)

14 The right sort of woman to start a dame school (3)

18 "The War" (anag) (6)

19 When hammering take care to hit this (two words)–5,4)

20 Making sound as a bell (8)

21 Half a fortnight of old (8)

23 Bird, dish of coin (3)

25 This sign of the Zodiac has no connection with the Fishes (6)

26 A preservative of teeth (6)

29 Famous sculptor (5)

30 This part of the locomotive engine would sound familiar to the golfer (5)

图 51:“每日电报”上的填字游戏用来作为新解密者的招募考试(答案见符录 H)。

了一个“炸弹”工作站。作为招募的一个途径,政府密码学校在杂志《每日电报》上刊登了一封信。他们匿名给读者提出一个挑战性问题,要求读者在12分钟内解决报纸上的填单词游戏(图51)。他们认为填单词游戏高手可以成为好的密码破解员,并补充布莱切里现有的科学思维,当然这些在报纸上没有提及。25个回信的读者被邀请到弗利特街进行一次填单词测试,有5个人在规定的时间内完成了题目,另一个在12分钟还剩下一个。几个星期后,所有6个人受到军方情报人员的面试,并被吸收为布莱切里庄园的密码破解者。

截获密码簿

这一章谈到现在,恩格玛密码通讯已被公认为一项巨大的通信系统。但实际上,此系统有几个不同的网络。例如,北非的德国陆军拥有自己单独的网络,并且他们的恩格玛操作员的密码簿不同于在欧洲所用的。因此,如果布莱切里成功地辨认出日密钥,那所有从北非发出的德国情报将能够译解,然而北非的日密钥对破解欧洲传送的情报是无用的。同样,德国空军也有自己的通讯网络,要破解所有德国空军的通信,就不得不揭开德国空军的日密钥。

有些网络比其他网络更加难于破解。德国海军网络是所有网络中最出色的一个,因为德国海军操纵着一个更复杂版本的恩格玛机。例如,海军恩格玛操作员有八个扰频器的选择,而不是五个。这就意味着德国海军的恩格玛机有几乎六倍于普通恩格玛机的扰频器排列,因此就有几乎六倍的密钥需要布莱切里测试。海军的恩格玛的另一个不同在于反射器。它负责通过扰频器把电信号发送回来。在标准的恩格玛中,反射器通常安置在一个特定的

方向,但海军恩格玛的反射器可能安置在 26 个方向的任何一个。由于这个因素,密钥的可能数量就进一步提高了 26 倍。

德国海军的操作员更使得海军的恩格玛难于破解。他们非常小心,从不发送陈旧的信息,那么布莱切里就很难发现克利巴。而且,德国海军创立了更安全的系统,用于选择和传递信息密钥。额外的扰频器、多样的反射器、新异的信息和一个新的用于交换信息密钥的系统,这些都使破译德国海军的通信难上加难。

布莱切里破解海军恩格玛的努力终于失败了。这意味着德国海军正在逐步取得大西洋战争的优势。海军上将卡尔·多尼兹为海战已经发展出一种高效的双阶段策略。一开始,他的德国潜艇散布穿梭于大西洋,寻找盟军的护航舰队。一旦某只潜艇发现目标,就展开下一阶段的行动。它呼叫其他潜艇到达目的地。当大批的潜艇准备就绪,进攻就将开始。为了确保联合袭击的成功,德国海军取得安全的通信信息就至关重要。海军的恩格玛正好提供了这种安全的通信。盟军的海上航运提供给英国人必需的食物和武器,德国潜艇的袭击却给它以毁灭性的打击。

由于德国潜艇的通信秘密化,盟军就没有办法确定潜艇的位置,就不能为护航制定安全的航线。在 1940 年 6 月与 1941 年 6 月之间,盟军平均每月损失 50 艘船,盟军正处于险境,不能迅速建造新船来取代损失的船只。除此之外,在战争中还失去了 5 万名海员。一时间让人感觉英国海军部查明要德国潜艇踪迹好像只有一种策略,就是寻找英国沉船的位置。如果不能彻底地减少这些损失,英国人就有输掉大西洋战争的危险,这也就意味失去了整个大战。

波兰的经验与施米特事件告诫布莱切里机构,如果在破解密码这种智力斗争中失败,就需要依赖间谍、潜入和盗窃等手段,来获取敌人的密钥。有时候布莱切里会有一定的突破来对抗海军的恩格玛密码,这也得感谢皇家空军的聪明策略,英国飞机在特定的

地方布置水雷，迫使德国舰船发出警告信号。这些恩格玛密码的加密警报将不可避免的含有一个地图信息，这个地图信息一旦为英国人所知，就可以被用作为一个克利巴，也就是布莱切里知道该密码一些特定部位代表一套坐标。以上散布地雷，获得克利巴的行动被称为“播种行动”，但这属于皇家空军特别的飞行行动，因此这样的信息就不可能有规律收集，布莱切里就不得不想出其他办法来破解海军的恩格玛。

另一种破解海军恩格玛的策略就是偷密钥了。伊恩·弗莱明和一群海军情报员策划了偷密钥的计划。这是最勇敢的计划之一。伊恩·弗莱明建议在英吉利海峡将已缴获的德国轰炸机故意坠毁在德国舰船的附近，德国海员就会靠近飞机营救他们。到时由英国飞行员假扮的德国人，到船上将密码簿偷取到。这些密码簿含有建立加密密钥所需的信息。并且德国舰船通常要离开基地很长时间，密码簿一般来说至少一个月内是有效的。通过获取这样的密码簿，布莱切里就能够在整整一个月内破解德国海军的恩格玛密码。

弗莱明的计划称为“冷酷行动”。在证实了该计划行之有效后，英国情报人员开始准备一架德国轰炸机，组织一队会说德语的英国机组人员。计划安排在当月开始，以便获取新的密码簿。弗莱明去了多佛监督这次行动，但遗憾的是没有德国战船在海上，所以这项计划被不定期的延迟了。弗兰克·伯奇是在布莱切里的海军分队的长官，他记载了四天以后图灵和他的同事彼特·特温听到计划取消后的反应：两天前图灵和特温走向我就像两具僵尸，他们还都沉浸在冷酷行动被取消的焦虑之中。

预期的冷酷行动被取消了，但在对德国气象观测船和潜艇的无数次勇敢袭击中，最终获得了德国海军的密码簿。这个密码本给了布莱切里必要的信息，把中断的情报连接起来。通过监测德国海军的信息传送，布莱切里就能够确定德国潜艇的位置，这样大

西洋战争开始向有利于盟军的方向发展。护航舰队能迅速改变航线,以躲避德国潜艇。英军的驱逐舰也开始展开攻势,搜寻并击沉德国潜艇。

德国最高司令部从没怀疑过盟军已经窃取了恩格玛密码簿。这是至关重要的。如果德国人发现他们的安全受到了威胁,他们将升级恩格玛机,那么布莱切里就会回到原来的状态。就像齐默尔曼电报事件那样,英国人同样采取了各种措施避免德国人的怀疑,例如盗取密码簿后击沉该德国舰船。这样德国海军上将多尼兹就会相信,密码材料已经沉入了海底,而不是落入了英国人的手里。

材料秘密地获取,在利用取得的情报之前,还要有进一步防范措施。例如,恩格玛解码提供了许多德国潜艇的情报,如果突然进攻每一个目标将是不明智的,因为这样的话英国人成功率的突然得到提高,可能会警告德国人他们的通讯已经被破译了。因此,盟军会允许一些德国潜艇逃脱,并且在开始进攻前,先派遣侦察机侦察一下。这样就使德国人相信英军是在侦察机发现情况后才发动了袭击。或者盟军也可发送他们观察到德国潜艇的假情报,就为袭击提供了充分的理由。

尽管这些策略把恩格玛被破解的迹象减小到了最少,但英国人的行动有时也使德国安全专家提高警惕。有一次布莱切里破解了恩格玛的信息,得到了一组德国潜艇和运输船的位置。为了减少德国人的怀疑,在大清扫行动中海军部并不想击沉所有的船只,他们发送给驱逐舰的信息中,只包括九艘舰船中七艘的精确位置,他们想让其他两艘“格达尼亚”和“宫泽海姆”号安全逃脱。但皇家海军的驱逐舰在击沉了七个目标之后,又巧遇了另外两艘船,并击沉了它们。舰上的海员不知道恩格玛这回事,也不知其中的策略,知道这是他们的职责。消息传回了柏林,海军上将库尔特·弗里克调查了这个事件及其他类似袭击事件,仔细地研究了恩格玛被破

解的可能性。调查报告表明大量的损失是由于自然的不幸，或是英国间谍渗透到德国海军的结果，德国人认为破解恩格玛是不可能的，那是难以置信的。

神秘的密码破译者

成功破译了德军密码后，布莱切里又开始破译意大利和日本的电文。为方便破译这三国的密电，英军成立了一个叫“乌特拉”的组织。乌特拉负责向盟军提供北非各主要战场上清晰的形势分析。在战争中，乌特拉帮助盟军摧毁了德军的供给线，获取德军在鲁麦尔的兵力情报，使英军击溃了德军精锐部队。乌特拉也预先警告了德军对希腊的侵略，这帮助英军成功地从希腊撤兵而没受什么大的损失。事实上，乌特拉对德军在整个地中海行动都作了准确地报道。这些信息在 1943 年盟军登陆意大利和西西里岛时作用尤为突出。

1944 年盟军在欧洲大陆反攻战中，乌特拉也发挥了重要作用。如，在“D”日计划实施的前一个月，布莱切里的译文提供了德军在法国边界集结的详尽态势。研究战时英军解密问题的历史学家哈里·欣西雷先生这样写道：

> 随着乌特拉的壮大，它执行了一系列令人震惊的行动。特别是它揭示了德军“五月行动”中的第二部分计划——此前德国人的扰乱计划使盟军认为勒阿弗尔和瑟堡之间的地带是一个最有可能的甚至是主要的进攻地区——第二部分计划揭示德军实际准备增援诺曼底和瑟堡半岛。但是，这些消息被及时送给盟军总部，帮助盟军及时修正由其他海岸登陆的作战计划。在盟军先遣队出发

之前，乌特拉还修正了盟军原先持异议的关于敌军在西部各师人员、特点和位置的估计文件，认为其 58 条中绝大部分是准确的，并且其中两条对军事战略有决定性意义。

在整个战争中，布莱切里的电码译员知道他们的破译是至关重要的，这种观点在丘吉尔亲自造访布莱切里时变得更加强烈。但是这些密码专家并不知道那些破译的译文具体有何作用。例如，这些电码译员并不知道 D 日计划执行的具体日期，而在登陆的前一天晚上他们还被安排去参加舞会。当然这令布莱切里的最高长官特拉维斯很不安，因为他是惟一的知情者。但他不能告诉舞会组织者取消这一舞会，因为他不能对在近海即将进行的这场大规模战争作任何暗示，那可是绝密的计划。舞会只得照常进行，不过后来由于天气原因，登陆战被迫推迟 24 小时，电码译员才得以从舞会的兴奋中回转过来。登陆那一天，法国军队切断了德军的陆上通讯线，德军只得完全依靠电波联络，布莱切里正好趁此机会大量截取并破译德军信息。在战争的关键时刻，布莱切里给盟军提供了敌军更具体的军情。六位破译专家之一的斯图尔特·米尔纳·巴里就曾写到：“我不敢想像从古到今有哪一场战争像现在这样，它是在一方知道对方的各种军情下进行的。”另一位美国记者也有相同感慨：“乌特拉极大地影响了高级参谋和政府要员制定计划的决策，使他们改变了一些决定。当你想到你对敌人了如指掌时，这种感觉是多么痛快。如果你能随时知道对手的想法、习惯和行动，那么洞察对方的能力随着时间的推移将会慢慢增强。这方面的信息也会使你自己的计划少一些盲目而多一些安全感，计划实施起来也少一些伤害而多一些轻松。”

布莱切里的成功是不是盟军最终获得胜利的决定因素还仍有争议，但这仅仅只是争议而已。有一点可以肯定的是，布莱切里的

密码破解员加快了这场战争的结束。只要想想如果没有乌特拉的支持大西洋战争会是什么样的情形，布莱切里的作用就显得更加重要。在大西洋战争中，德军潜水艇占据了优势，盟军损失了大量的船只和供给物，甚至严重危及了美国的国家安全，同时，盟军不得不投入大量人力和物力去建造新船。历史学家估计仅仅是因为造船就会使盟军的计划推迟了好几个月，这也意味着"D"日计划将会可能被推迟到次年。米尔纳·巴里曾说："如果政府密码学校不能破解德军电文，没有乌特拉的出现，二次世界大战不会在1945年结束，而是1948年。"

在延误的这段时间里，又将有更多的人在欧洲战场牺牲。希特勒会更大量地使用武器，造成南部英格兰的恐慌。为尽快结束战争，减少人员牺牲，这不仅是同盟军的，也是苏联人、德国人、意大利人、日本人等的共同心愿，就连历史学家大卫·卡恩也高度赞扬了破译密文这一做法。二战幸存者认同这一做法。这些密码破译员给全世界的人带来恩惠。

战后，英国仍然保密对布莱切里破译德军密码的成就，英军是如何破译电文的仍然没人知道。英国想继续这方面的工作，并且不愿意透露其在破译密码方面的能力。事实上，战争结束后，英国掌握了成千上万台恩格玛密码机，并把这些机器分发给它的那些前殖民国家，这些前殖民国家与德国人一样一直以为这样的密文是不可能被破译的。在随后的几年里，英国照例对密文的事保持沉默，并照常进行他们的解密工作。

同时，英国关闭了在布莱切里院的密码破译机构和密码破译学校，在战争中曾经对乌特拉作出过巨大贡献的成千上万的人员也被裁减了。二战时破译密文相关的旧资料不是被封存起来就是被烧了。电文破译组织被改名为政府通讯总部(GCHQ)，地址在伦敦，于1953年后又搬到切尔滕纳姆。虽然一些破译专家进了政府通讯总部，但大多数人过着平民生活，宣誓保守秘密，不能泄露

他们在二战中所扮演的关键角色。当那些参加常规战争的人谈论他们英雄事迹的时候，这些战时参加破译工作的人——毫无疑问是非常重要的的人——在谈论他们的战时活动时却是非常尴尬。戈顿·韦尔什曼就曾叙述说："有个跟他在6号屋一起工作过的年轻破译专家曾收到老校长的信，指责他没有上前线，给学校丢了脸。"德里克·汤特同样在6号小屋工作过，在总结他和他同事们的真正贡献时说："我们在圣克里斯宾的日子可能没有和金·哈里一样悲伤，但我们确实并没有躺在床上，我们没有理由因为自己曾经工作的地方而受指责。"

在经历了30年的沉默后，1970年代初布莱切里大院的秘密终于公布于众。当年曾负责解散乌特拉组织的温特博特姆上将开始给英国政府施加压力，认为联邦政府应该停止破译恩格玛密码，继续隐瞒当年英军成功破译德军密文的事实已不会给英国带来任何好处。有关部门只得勉强同意，并且允许他写一本关于布莱切里大院的书，公开布莱切里大院的秘密。1974年夏温特博特姆上将写的《乌特拉的秘密》一书正式出版，这也意味着那些当年在布莱切里庄园工作过的人现在可以谈论他们在战时的事迹。戈顿·韦尔什曼就对此感到如释重负，他说："战后这么多年来我一直在回避战争中的那些事情，因为这很容易在有意无意中暴露乌特拉的一些事情……现在事情的转变终于把我从那时保守秘密的誓言中解放出来了。"

那些在战争中作出过巨大贡献的人终于得到了他们应该得到的荣誉。温特博特姆上将批露出布莱切里大院事实的最大后果，也许是雷白斯基终于意识到他战前破译恩格玛所带来的结果。在德军入侵波兰后，雷白斯基逃到了法国，法国沦陷后又逃到不列颠。随后就顺理成章的为英军破译密文服务，但他却被分人靠近赫米尔-享普斯特德的博克斯木尔镇的一个小密码研究所中负责译员后勤工作。至于这样一位才华横溢的密文专家为什么没有被

布莱切里庄园收录,其原因尚不清楚,雷臼斯基也不知道密码破译机构和密码破译学校的存在。直到温特博特姆的书出版,雷臼斯基才了解他战前所取得的突破是英军后来破译密文的基础。

对有些人来说,温特博特姆的书出版还是来的迟了些。布莱切里的第一任领导阿拉斯泰尔·丹尼斯顿的女儿在他父亲死后多年收到一封他父亲同事的来信,信上说:"你父亲是一位真正伟大的人,所有了解他的人都会记住他的,甚至到永远。惟一令人遗憾的是理解他所做工作的人太少了。"

阿兰·图灵是另一个不幸的破译专家,他没有活到人们认同他的时刻,他不仅没有获得"英雄"称号,还因为同性恋的原因而遭受迫害。1952 年在一次被警察传讯中,他天真地透露他是同性恋。警察认为别无选择,根据 1885 年通过的刑法修正案第十一部分的反猥亵条例对他进行了起诉,新闻界也大肆炒作,搞得图灵身败名裂。

图灵秘密被曝光后,他的个性也是尽人皆知。英国政府撤回给他的各种保障,他也被迫在与计算机发展相关的研究领域工作。后来他被强迫向心理学家咨询,并且承受着外来的各种指责,这些都使他变得肥胖而虚弱,两年后他变得更加消沉。在 1954 年 7 月 7 日,他带着一瓶氰化物和一个苹果走进自己的卧室,20 年前他常唱邪恶女巫的歌谣:"将苹果放在毒药里蘸一下,让睡神悄悄来临。"现在他决定遵照她的咒语去做。他将苹果放在氰化物里蘸了蘸,咬了几口。就这样一个真正的破译天才在他年近 42 岁时,自杀了。

第五章 语言上的隔阂

英国的电文译码员破解了德国的恩格玛密码，并因此扭转了欧洲战场的战局。而与此同时，美国电文译码员在太平洋战区也起到了同样重要的作用。他们破解了被称为“紫色”的日本机器密码。1942 年 6 月美国人破译了日本海军的一条电文。根据这条电文，美国人得知日本海军计划佯攻阿留申群岛，以吸引美国海军军力，从而可以进攻真正的目标——中途岛。美国海军将计就计，将舰队调离中途岛，在附近海域徘徊。当美国密码破译员截获并破译出日本军队进攻中途岛的命令后，舰队立即回航，保卫中途岛。这一战役是整个太平洋战争中最重要的几次战役之一。据海军上将切斯特·里米茨说，中途岛胜利归功于美军的智慧。日军本想打美国一个冷不防，结果自己反而措手不及。

大约一年后，美国密码破译员辨别出一条电文，电文中透露了日本舰队总司令海军上将山本五十六去视察北所罗门群岛时的飞行路线。里米茨决定派出战斗机去拦截山本五十六的飞机，并将它击毁。以守时闻名的山本早上 8 点就准时到达目的地，和电文中所透露的一样。迎接他的是 18 架美国 P－38 战斗机。他们成功地击毁了这个日本高层指挥官中最有影响力的人物的座机。

虽然，德国的“恩格玛”密码和日本的“紫色”密码最终被破解，

然而,它们刚问世时确实起到了安全通讯的作用,也给英国和美国的密码破译员提出了很大的挑战。实际上,如果解码机没有被正确的使用;没有重复的电文密钥;没有克利巴;没有对线路连接板和加密器安置的限制以及没有固守陈套的电文(从中可以推出译码表)——它们有可能永远不会被破解。

英国军队所用的 Typex(或 Type X)加密机和美国军方的 SIGABA(或 M-143-C)加密机显示了机器加密的潜在实力。这两种机器都比恩格玛密码机更为复杂,由于得到了正确的使用,以致于到战争结束它们都还没有被破解。盟军的密码破译员相信复杂的电动机械加密机能够保证通讯的安全。虽说如此,复杂的加密机并不是能够发送安全信息的惟一途径。实际上,二战中所用的一种最安全的加密方式恰恰是最简单的一种。

在太平洋战役期间,美国指挥官意识到像 SIGABA 这样的加密机存在一个根本的缺陷。虽说电动机械加密法提供了相对较高的安全性,然而它的费时是让人痛苦的。电文逐字输入到机器中,机器逐字输出加密文字,然后,无线电发报员发出整篇加密文字。对方接收到加密文字后,送到密码专家的手中,密码专家谨慎的挑选好密码钥,并把密码文字输入到机器中,机器逐字输出解码文字。在指挥部或者在船甲板上倒是有充裕的时间和足够的空间来进行这么一项精密的工作。然而,在更糟糕的环境中,比如在太平洋的小岛上,机器加密显然是不太适合的。一个战地通讯员是这样形容在一场生死攸关的激战中对通讯的困难的:“当战斗被限定在一个非常小的地方,每时每刻战局都在不停的变化,根本没有时间编码和解码。在这种时候,我们采用土话通讯,越土越好。”不幸的是,许多日本士兵上过美国大学,他们对美国土话也非常熟悉,美军有价值的战略和战术信息就这样落人敌人的手中。菲利普·约翰斯顿是最早对这个问题作出反应的人之一,他是洛杉矶的一名工程师。

由于约翰斯顿岁数太大而不能参军，但他仍然想为战事作出点贡献。1942 年初，他受到儿时经历的启发，开始设计一套加密系统。作为新教传教士的儿子，约翰斯顿成长在亚利桑那州的纳瓦霍族保留地，结果他完全沉浸于纳瓦霍文化中。他是少数可以说流利的纳瓦霍族语言的非纳瓦霍人之一，因此他成为了纳瓦霍人与政府之间对话的翻译。在约翰斯顿 9 岁的那年，两个纳瓦霍人在白宫为他们的居民向西奥多·罗斯福总统恳请得到更公平的对待，而他就是当时的翻译，这是他翻译事业的顶峰。约翰斯顿充分意识到外族人理解纳瓦霍族语言的困难，一个想法在他的脑中渐渐形成。纳瓦霍族语言或者任何一种美国土著语，是否可以被用为一种不能破解的密码呢？如果太平洋战区的每一支军队雇佣两个美国土著人作为无线电收发员，就完全可以实现安全通讯了。

带着他的想法，他去会见了埃里欧特营地的通讯指挥官陆军中校詹姆斯·E·琼斯。这个营地就在圣迭戈外边。仅仅向这位疑惑的指挥官说了几句纳瓦霍话，约翰斯顿就成功地说服了他，使他开始认真考虑这个建议了。两个星期后，约翰斯顿和两个纳瓦霍人再次来到这个地方，这一次，他们准备在海军高级将领面前做一次测试。纳瓦霍人被隔离在两处，给其中一个人用英文写的六条典型电文，然后，让他翻译成纳瓦霍语并传送给另一个纳瓦霍人，他再把这六条电文翻译成英文。海军将领对比了翻译过两次的电文和原始电文。事实证明纳瓦霍人在这次测验中的表现是完美无缺的。海军拟定了一个"领航员"计划并且下令立即开始招收新兵。

但在招收任何人之前，陆军中校琼斯和詹姆斯·约翰斯顿必须先作出一项决定，就是让"领航员"说纳瓦霍语呢还是选择另一个土著语言。约翰斯顿一开始用纳瓦霍人说明他的想法，是因为他和这个部落有私交，但这不意味它就是最理想的选择。选择的标准简单来说有几个因素：海军要找到一个土著部落有足够的人既

能说流利的英语又能说土著语。缺乏政府的投资意味着在保留地之外很少人会这种语言。这样,注意力就集中在四个最大的部落:纳瓦霍、苏人、齐佩瓦族和佩玛-帕帕笱。

纳瓦霍的人数最多,但读写能力最差,而佩玛-帕帕笱的读写能力最好,人数却少的多。总体来说,四个部落相差不大。最终的决定取决于另一个重要的因素,它来自于针对约翰斯顿的想法作出的官方报告:

纳瓦霍族是近20年来惟一一个没有被德国学生侵染的部落。德国人伪装成文科学生、人类学家等身份,来学习各个部落的方言。无疑除了纳瓦霍族以外,他们已经获得了各种方言的知识。因为这个原因,纳瓦霍是惟一一个能保证这项工作绝对安全的部落。而且另一个因素是除了受过这种语言训练的28个美国人,别的部落和其他人都不懂得纳瓦霍部落的语言。这种方言对敌人来说相当于密码,因此非常适合用作快速安全通讯的手段。

美国参战时,纳瓦霍族人的生活条件非常坚苦,他们被看成低等人。然而,他们部落仍然支持美国参战,并且表示了他们的忠诚:"再没有比美国本土人更爱美国的了。"纳瓦霍人渴望参战,为了参战,他们谎报年龄,甚至在称体重前喝大量的水以达到55公斤的合格线。所以,要找到纳瓦霍通讯员的志愿者并不困难。珍珠港事件4个月后,29名纳瓦霍人开始在海军中接受为期8星期的通讯课程训练。他们当中有的年仅15岁。

在训练开始之前,海军必须克服一个问题。这个问题困扰着另一个基于美国土著语的密码系统。第一次世界大战在法国北部,141团D连的陆军上尉E·W·霍纳曾经雇用了8位乔克托族人作为无线电收发员。当然没有敌人可能理解这种语言,所以用乔克托语通讯是很安全的。可是,这种加密系统有本质的缺陷,因为,乔克托语中没有现代军队的行话。电文中的专业术语常被翻译成具有歧义的乔克托语,接收者很可能产生误解。

在纳瓦霍语中也存在同样的问题，因此，海军决定构造一个纳瓦霍语的专业术语词汇表，以消除这种歧义。受训的纳瓦霍人协助构造了这个词汇表，他们倾向于选择描述自然世界的词汇来表示特定的军队用语。飞机用鸟的名字表示，而舰船用鱼的名字表示(见表 11)。指挥官叫做“战争酋长”，排则叫做“泥巴部落”，要塞叫做“洞巢”，迫击炮被命名为“蹲着的枪”。

虽然整个词汇表中有 274 个单词，但要翻译人名、地名以及一些难料的单词仍然很困难。解决方法是根据语音设计了一个加密的字母表，用它来拼出难词。比如，单词“Pacific(太平洋)”可以用这种方式拼出来：“pig(猪)，ant(蚂蚁)，cat(猫)，ice(冰)，fox(狐狸)，ice(冰)，cat(猫)”。翻译成纳瓦霍语就是“bi - sodih，wol - la - chee，moasi，tkn，ma - e，tkin，moasi”。

表 11：纳瓦霍密码中的飞机和船

Fighter plane	Hummingbird	Da-he-tih-hi
Observation plane	Owl	Ne-as-jah
Torpedo plane	Swallow	Tas-chizzie
Bomber	Buzzard	Jay-sho
Dive-bomber	Chicken hawk	Gini
Bombs	Eggs	A-ye-shi
Amphibious vehicle	Frog	Chal
Battleship	Whale	Lo-tso
Destroyer	Shark	Ca-lo
Submarine	Iron fish	Besh-lo

表 12 中是完整的用纳瓦霍语表示的字母表。受训者在 8 个星期内就学会了整个词汇表和字母表，他们甚至不需要密码簿，这样就消除了密码簿落入敌人手中的危险。对于纳瓦霍人，记住这些密码是很简单的一件事。因为他们的语言传统上是没有文字的，所以他们习惯于用大脑记住他们的民间故事和家族历史。一

个受训的纳瓦霍人威廉姆·麦凯比说："在纳瓦霍，每件事都在记忆中——歌、祈祷以及所有的东西。我们就是这样被养大的。"

训练结束后，纳瓦霍人接受了一次测试。电文发送者将一系列的电文翻译成纳瓦霍语后发送给接收者，接收者将电文翻译成英文，并在必要时用到记忆中的军事术语词汇表和字母表。结果是完美无缺的。为了检验这个密码系统，一份录有电文传输讯号的录音带送到了海军情报局。他们曾经破解了最难的日本密码"紫色"。经过三个星期高强度的密码破译后，海军密码破译专家仍然对这些电文困惑不解。他们称纳瓦霍语是"一系列奇怪的喉音、鼻音和卷舌音的组合……我们甚至不能把它记录下来，更别说破解它了。"纳瓦霍密码被证明是成功的。两位纳瓦霍士兵约翰·本纳尼和约翰尼·曼纽莱托留下来训练下一批人员，另外27名纳瓦霍密码通讯员则被分为4组派遣到太平洋上去了。

表12：纳瓦霍字母表密码

A	Ant	Wol-la-chee	N	Nut	Nesh-chee
B	Bear	Shush	O	Owl	Ne-ahs-jsh
C	Cat	Moasi	P	Pig	Bi-sodih
D	Deer	Be	Q	Quiver	Ca-yeilth
E	Elk	Dzeh	R	Rabbit	Gah
F	Fox	Ma-e	S	Sheep	Dibeh
G	Goat	Klizzie	T	Turkey	Than-zie
H	Horse	Lin	U	Ute	No-da-ih
I	Ice	Tkin	V	Victor	A-keh-di-glini
J	Jackass	Tkele-cho-gi	W	Weasel	Gloe-ih
K	Kid	Klizzie-yazzi	X	Cross	Al-an-as-dzoh
L	Lamb	Dibeh-yazzi	Y	Yucca	Tsah-as-zih
M	Mouse	Na-as-tso-si	Z	Zinc	Besh-do-gliz

1941年12月7日，日本军队偷袭珍珠港。此后不久，他们控

制了西太平洋的大部分地区。12 月 10 日,日军侵入了关岛的美军要塞。12 月 13 日,他们占领了瓜达康纳尔岛——所罗门群岛之一。12 月 25 日,香港被占。1942 年 1 月 2 日,菲律宾的美军投降。同年夏天,日军计划在瓜达康纳尔岛上建立一个机场以加强对太平洋的控制。这个轰炸机基地使他们能够摧毁盟军的补充航线,这样的话,盟军就不可能做任何反击了。美国海军司令欧内斯特·金上将下令在机场完工前进攻瓜达康纳尔岛。8 月 7 日,第一海军舰队作为先锋开始攻击瓜达康纳尔岛。在最初登陆的部队中就可以看到纳瓦霍密码通讯员的身影,这是他们第一次参加作战。



图 52:第一批 29 纳瓦霍密码解译班准备好照传统毕业照的姿式。

虽然纳瓦霍人相信他们的技术将使海军受益非浅,然而他们的第一次尝试带来的只是混乱。很多常规的通讯员不了解这种密码,他们甚至认为这是日本军队的密码电文,所以,他们非常惊恐

地发布消息说日本军队正在用美军使用的频率通讯。当勤的上校立即中止了使用纳瓦霍语通讯,直到他说服自己这个系统是值得信赖的,他才恢复了纳瓦霍语通讯。一个密码通讯员回忆纳瓦霍语通讯是怎样恢复的,他说:

> 上校有一个主意。他说他可以保留我们,但是我必须跟他的"白色密码"—— 一个圆柱状的密码机器比赛并且赢了它。否则,我们只能卷铺盖走人。机器和我都发出电文,然后,我们分别得到了上校的回答。比赛是看谁先解码出上校的回答。我被问道,"你需要多长的时间?""两分钟多。"我回答道。当另一个小伙子还在解码时,我已经收到对我做出的回答了。而这一切仅仅花了4分半钟。我问上校:"上校,你什么时候放弃那个圆柱状的玩意儿?"他没有回答,只是点燃了他的烟斗,走开了。

密码通讯员很快证明了他们在战场上的价值。在塞班岛的一次战役中,一队日军撤退后,海军某营占领了原先由他们把守的位置。突然,一声巨响,一枚炮弹落在附近。他们正受到另一队美军的炮击,那队美军根本没注意到他们前进的这么快。他们通过无线电通讯用英语说明了他们的情况,然而,炮击仍在继续。因为进攻的美军怀疑这电文是日本人模仿的,想骗他们。直到他们接收到一个纳瓦霍语的电文,他们才认识到自己的错觉,停止了攻击。纳瓦霍电文是无法伪造的,而且永远可以信赖。

密码通讯员声名鹊起。到 1942 年末,又需要征召 83 名密码通讯员。纳瓦霍人在所有的六个海军舰队服役,而且有时候还被其他的军队借用。纳瓦霍人的"战场上的语言"很快使他们成为英雄,其他士兵自愿为他们背发报机、扛枪,他们甚至有了自己的私

人保镖，受到战友的保护。但密码通讯员常因被误认作是日本兵而被美军俘虏，只有他们同营战友来为他们担保后，他们才得以释放。这种情况至少出现了三次。

纳瓦霍语是纳迪尼语系的一种，这个语系与欧洲和亚洲的语言毫无关联。这是纳瓦霍语密码难以理解的原因。比如说，纳瓦霍语的动词不仅跟它的主语有关，而且还跟宾语有关。动词的后缀决定于宾语的种类。这些种类包括长的（例子：管道、铅笔），细长的、柔软的（例子：蛇、皮带），颗粒状的（例子：糖、盐），束状的（干草），粘的（例子：泥巴、粪便）等等。动词也常常和副词结合在一块儿，而且动词本身反映了说话人对他所说的事情的熟悉程度，他是不是道听途说。结果是，一个动词就相当于一个句子。一个外族人想弄明白它的意思，几乎是不可能的。

虽然纳瓦霍语密码很强大，但它仍有两个重大的缺点。首先，既不在纳瓦霍语土语词汇又不在官方认定的军事术语词汇表中的单词，必须用特殊的字母表拼出，这是个耗时的工作。所以，决定再向术语词汇表中添加 234 个常用词汇。举例说，各个国家都冠以了纳瓦霍语的别称：澳大利亚叫“滚动的帽子”，英国叫“被水包围着”，中国叫“编起来的头发”，德国叫“铁帽子”，菲律宾叫“漂流着的陆地”；而西班牙叫“痛苦的绵羊”。第二个问题是关于那些不得不拼出来的单词。如果日本人意识到单词是拼出来的，他们用频率分析法很容易判断哪个纳瓦霍单词代表哪个字母。很快就可以发现最常用的纳瓦霍单词是 dzeh，它的意思是麋鹿（英文是 elk），代表英语中最常用的字母 e。而拼一下岛的名字瓜达康纳尔（Guadalcanal）就会发现其中有 4 个 a，而这是推出 4 个重复的单词 wol - la - chee（ant 蚂蚁）代表 a 的重要线索。解决的方法是增加更多的单词来代表同一个常用字母。于是，最常用的六个字母（e，t，a，o，i，n）各增加了 2 个额外的单词代表。次常用的六个字母（s，h，r，d，l，u）各增加了 1 个额外的单词代表。这样，Guadalcalnal 可以被拼为：klizzie，shi - da，wol

– la – chee, lha – cha – eh, be – la – sana, dibeh – yazzie, moasi, tse – nihl, nesh – chee, tse – nihl, ah – jad(goat 山羊, uncle 叔叔, ant 蚂蚁, dog 狗, apple 苹果, lamb 羊羔, cat 猫, axe 斧子, nut 坚果, axe 斧子, leg 腿)。其中只有一个重复的单词。

随着太平洋战争的推进,美军从所罗门群岛进攻到冲绳岛,纳瓦霍密码通讯员扮演着越来越重要的角色。在进攻硫黄岛的前几天,共发送了八百多条纳瓦霍密码电文,而且无一失误。据少将霍华德·柯纳说:"如果没有纳瓦霍人,美国海军可能永远都攻不下硫黄岛。"



图 53:亨利·贝克下士(左)和一级列兵乔治·H·柯克 1943 年在布干维尔岛使用纳瓦霍密码。

纳瓦霍密码通讯员为了完成他们的使命,他们还不得不对抗他们心中深藏的恐惧,纳瓦霍人相信如果不对尸体举行特定的仪式,死亡的幽灵陈迪会向活人复仇。太平洋上的战争是血腥的,战场上横尸遍野,密码通讯员必须鼓足勇气克服对陈迪的恐惧。考虑到这一点,纳瓦霍通讯员就更加卓越非凡了。在多瑞仕·保尔的《纳瓦霍密码通讯员》一书中,一位纳瓦霍人讲述了一个故事,它非常典型地反映了他们的勇气、沉着和献身精神:"如果你把你的脑袋再抬高6英寸,你就完了,火力是这么猛。在凌晨的时候,无论是我们这边还是敌人那边都丝毫不能放松,只有死一般地间歇。一直是这样,所以才有一个日本人不能再忍受了。他站起来,用他最大的声音咆哮,冲向我们的战壕,挥舞着一把长长的武士刀。我猜想他在倒下前中了25到40枪。"

"在战壕中,有一个伙伴在我旁边。他被日本人割穿了喉咙,一直割到他脖子后面,他仍然在通过他的气管喘息。他呼吸的声音是如此的可怕。当然,他最终是死了。当日本佬进攻时,热血溅满我握着话筒的手。我在用密码求救,他们告诉我,无论发生了什么,我电文的每一个音节都得传出。"

总共有420名纳瓦霍密码通讯员。虽然他们作为战争的英勇被得到了承认,然而,他们在安全通讯中的特殊角色被归属机密。政府不准他们谈论他们的工作,他们独一无二的贡献却不为大众所知晓。就和图灵以及在布莱切里院工作的密码破译专家一样,纳瓦霍密码通讯员被忽视了几十年。终于,1968年政府撤销了纳瓦霍密码机密。次年,纳瓦霍密码通讯员举行了他们的第一次团聚会。1982年,政府将8月14日定为"纳瓦霍密码通讯员日",以表彰他们在二战中的贡献。然而,他们所作的最伟大的贡献是他们使用的密码是历史上为数不多的未被破解的密码之一。日本情报局局长静三有末中将承认即使他们破译了美国空军的密码,他们对纳瓦霍密码仍毫无办法。

破译失落的语言和古代的文字

纳瓦霍密码的成功大部分基于一个简单的事实，一种语言对于一个不熟悉这种语言的人来说是无法理解的。在许多方面，日本密码破译员所遇到的问题和考古学家碰到的问题有相似之处。考古学家试图破译一种长期被遗忘的语言，而它很可能是用一种绝迹的文字写成的。与日本密码破译员相比，考古学家的任务更加艰巨，比如说，日本人有来源不断的纳瓦霍语电文供他们分析，而考古学家得到的有用信息往往只是几小块残缺碑文。不仅如此，考古学家对古代文字所讲的内容毫无概念。而电文内容是军事密码破译员用来分析密码的常用线索。

破译古代文字看起来是那么没有希望。可是，仍然有许多人投身到这项艰巨的工作中。他们想要理解我们祖先的文字，能够说祖先的语言，进而，探讨他们的思想和生活。这种强烈的欲望使他们痴迷于工作中。《破译的故事》一书的作者莫里斯·波普很好地概括了这种破译古代文字的欲望："破译文字是最迷人的学问。不为人知的文字总带着一丝神秘，尤其是当这文字来自于遥远的古代时更是如此。而第一个揭开它的神秘的人，就会得到相应的荣耀。"

破译古代文字并不是密码制造者和密码破译者的"道高一尺，魔高一丈"的战争。因为即使有形如考古学家的密码破译者，但却没有任何密码制造者。那就是说，大多数情况要破译的古代文字并没有故意隐藏文字的意思。这一章的后半部分是讨论古代文字破译的。这可能有一点点偏离本书的主旨。不管怎样，古代文字破译的原理和传统的军事密码破译的原理在本质上是一致的。事实上，破译古代文字的挑战吸引了许多军事密码破译员。这很可

能是因为古代文字破译与军事密码破译相比有很大的转变，它给予人的更多是纯智力的谜题，而非军事挑战。换言之，破译古代文字的动力来自于好奇心，而非敌意。

破译埃及象形文字的故事是所有破译故事中最著名的，也可以说是最浪漫（尚存争议）的一个。几个世纪来，象形文字始终是一个谜，而考古学家所能做的也只是猜测它们的意思。然而，多亏了一段经典的密码破解的故事，象形文字最终被破译了。从此，考古学家能够读到叙述古埃及历史、文化和信仰的第一手文字资料。象形文字的破译在我们与几千年前的法老文明之间架起了一座桥梁。

最早的象形文字可以追溯到公元前3000年，而且从那以后这种华丽的书写持续使用了3500多年。虽然象形文字精致的书写符号非常适合刻在宏伟神殿的墙上（希腊词 hieroglyphica 的意思就是"神圣的雕刻"，而象形文字在英文中写作 hieroglyphics），但对于日常事务来说确实显得过于复杂。所以，有一种称为僧侣体（hieratic）的文字与象形文字并行演化。僧侣体是象形文字的简化写法，写法方便简单，用于日常书写中。到了公元前600年，僧侣体被一种更加简单的书写文字所替代。这种文字称作通俗体（demotic）。这个词来源于希腊文 demotika，意思是"流行"。这反映了它是用在世俗的地方。象形文字、僧侣体和通俗体本质上是同一种文字——它们仅仅是同一种文字不同的写法而已。

所有三种文字都是表音的，就是说每一个字主要是代表一个读音，就和英语中字母表中的字母一样。三千多年来，古埃及人在生活的方方面面使用这些文字，就像我们今天写字一样。然后，接近公元4世纪末，仅仅一代人的时间，古埃及文字消失了。最晚可确定年代的古埃及文字是在菲莱岛上找到的。它们分别是公元394年用象形文字所刻的神殿里的碑文和公元450年左右一片用僧侣体写的涂鸦。基督教的扩张应该对古埃及文字失传负主要责

任,为了消灭埃及的异教传统,基督教徒们宣布使用古埃及文字是不合法的。取代古埃及文字的是科普特(Coptic)。科普特是由 24 个希腊字母和 6 个通俗体字母联合组成,这 6 个通俗体字母补充了在希腊语中没有发音的古埃及语音。在科普特的强大统治下,人们失去了读象形文字和通俗体和僧侣体的能力。古埃及语仍在口语中使用,进而演化成了科普特语言。但是不久以后,也就是 11 世纪,随着阿拉伯语的传播,科普特语和它的文字被取代了。与埃及古国的最后的语言联系就这样中断了,读懂法老故事的知识消失了。

人们对象形文字的兴趣在 17 世纪复燃了。那时,罗马教皇赛可斯图斯五世根据一个新的街道图纸重新规划罗马城,他在每个十字路口树立了一个来自埃及的方尖碑。学者们试图弄懂方尖碑上的象形文字,但是基于一个错误的假设,他们很难有所进展。没有人会接受这些象形文字代表的是一个音。他们认为拼音文字对一个古老的文明来说过于先进了。所以,17 世纪的学者相信象形文字是表意符号。整个复杂的字代表的是一个概念,并不比原始的图画有更多的意思。甚至在古埃及文还在使用时,去过埃及的外国人也都这么想。狄奥多·西库鲁斯一位公元前 1 世纪的希腊历史学家这样写道:

> 埃及文字的形式来源于各种生物,人的四肢以及器皿的形状……因为,他们的写作并不通过符号的组合来表达更深的特定意思,而是通过符号复制什么东西或它的隐喻来表达……所以老鹰的符号对他们来说表示事情发生的很快,因为这动物几乎是飞得最快的鸟。通过一点隐喻,这个符号的意思就转变成所有迅速的东西和所有速度很快的东西。

在这种叙述的指引下,无怪乎17世纪的学者们试图通过解释每个字所代表的概念来破译象形文字。比如说,1652年,德国朱苏特牧师阿萨内修斯·基尔舍出版了一本比喻解释的字典,并用它作出了许多奇异美妙的翻译。我们现在已经知道仅仅是代表法老阿普瑞斯的名字的象形文字,被基尔舍翻译成:"要获得神圣的冥神奥西里斯的恩赐,必先举行庄严的仪式,献上鬼仆的锁链。这样,才能得到尼罗河的恩泽。"今天,基尔舍的翻译看起来是荒唐可笑的,但是它们对那些想成为破密码专家的人的影响是巨大的。基尔舍不仅是一名埃及学家。他写了一本关于密码术的书,并建造了一个音乐喷泉,还发明了一种魔术幻灯(电影的前身),他曾经亲自钻到维苏威火山的火山口中,被人称为'火山学家之父'。

基尔金是当时最受尊敬的学者,这一点得到了大多数人认同。而他的想法影响了一代又一代的埃及学家。

基尔舍之后一个半世纪,也就是1798年的夏天,古埃及的遗物再一次被学者们仔细研究。当时,拿破仑·波拿巴派遣了一队历史学家、科学家和绘图员尾随着他的侵略大军。这些学者被士兵戏称为"哈巴狗",然而他们作出了非凡的成就。他们制作地图,复制绘画,抄录文字,丈量土地,记录一切他们所见到的。在1799年,法国学者们遇上了考古史上独一无二的最著名的一块石板。这块石板是由驻扎在朱利恩要塞的士兵发现的。朱利恩要塞位于尼罗河三角洲的罗塞塔城。当时,这些士兵正在执行任务,他们摧毁古代城墙想要扩大要塞。建造在城墙中的是刻着重要文字的石头。这块石头上刻着分别用希腊语、古埃及通俗体和象形文字等三种文字书写的同一段碑文。罗塞塔之石看起来就相当于密码破译的双文对照,就和帮助布莱奇利庄园的密码破译员破解恩格玛密码的双文对照一样。拿容易读懂的希腊文与古埃及通俗体和象形文字比较,从中可以得到许多有用的信息。罗塞塔之石中藏有解开古埃及文字之谜的方法。

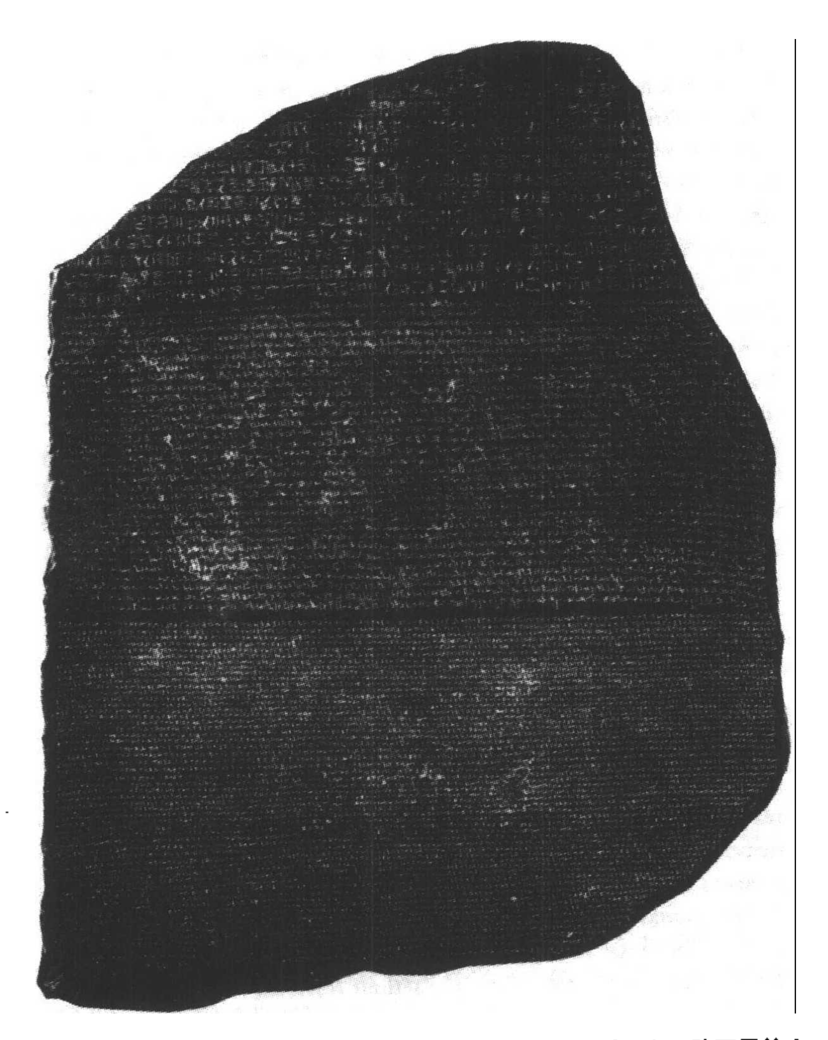


图 54:罗赛塔之石,刻于公元前 196 年,发现于 1799 年,由 3 种不同的文字所写,内容相同,其中象形文字在最上端,古埃及通俗体在中间,底端为古希腊文。

学者们立即意识到这块石头的重要性，它被送到开罗的国家学会去做详细的研究。但是，在学会做任何严肃的研究之前，法国军队已被英国军队逼得岌岌可危了。法国人把罗塞塔之石从开罗运到了相对较为安全的亚历山大。具有讽刺意味的是，法国人最后投降时，投降条约的第 16 条条款把在亚历山大所藏的古代遗物多数给了英国。而相反开罗的古代遗物却返还给了法国。1802 年，这块无价的玄武岩（118 厘米高，77 厘米宽，30 厘米厚，重 3/4 吨）被皇家海军舰船埃及号运往普利茅斯，同年它入住大英博物馆直至今日。

希腊文的翻译揭示了罗塞塔之石碑文的内容。它是埃及祭司最高会议于公元前 196 年颁布的布告。上面记录了法老托勒密赐福埃及人民，详述了祭司们作为回报给予法老的荣耀。比如说，他们宣布："每年 Troth 第 1 日的后五天，为仆塔神和埃皮法纳·尤卡里斯托神的宠爱，万寿无疆的托勒密国王举行盛大的节日，届时他们身着花圈，奉上牺牲和贡酒，和其他各种贡品。"如果其他两种文字记载的是同一个布告的话，破译象形文字和通俗体就是很简单的事了。然而，还存在着三个重大的障碍。首先，罗塞塔之石受损情况很严重（见图 54），古希腊文总共 54 行，其中后面的 26 行受损。古埃及通俗文字总共 32 行，开头的 14 行受损（注意象形文字和古埃及通俗文字是从右往左写的）。象形文字的受损情况最严重，几乎一半的文字全不见了，仅剩下 14 行文字（与希腊文的最后 28 行对应）也有部分缺失。破译文字的第二个障碍是已经至少有 8 个世纪没有人说过埃及文字所记录的古埃及语了。这样的话，即使考古学家可能把埃及文字与希腊单词对应起来，也不可能说出埃及文字的读音。最后的障碍是基尔舍的知识遗产仍然鼓励考古学家认为埃及文字是表意符号而非表音符号。因此，几乎没有人尝试着从语音上着手去破译象形文字。

英国天才博学家托马斯·杨是首先对象形文字是表意符号这

种偏见提出质疑的学者之一。1773 年,杨出生在萨默塞特的米尔弗顿。他两岁时就能很流利地读书。在 14 岁的时候,他已经学会了希腊文、拉丁文、法文、意大利语、希伯来文、迦勒底语言、古代叙利亚语、撒马利亚语、阿拉伯语、波斯语、土耳其语和埃塞俄比亚语。他在剑桥以马内里学院就学期间,卓越的才华为他赢得了"奇才杨"的绰号。在剑桥他学的是医学,但是据说他感兴趣的是疾病本身而非得病的人。渐渐地,他把精力更多地投入在研究上,照料病人的时候越来越少。

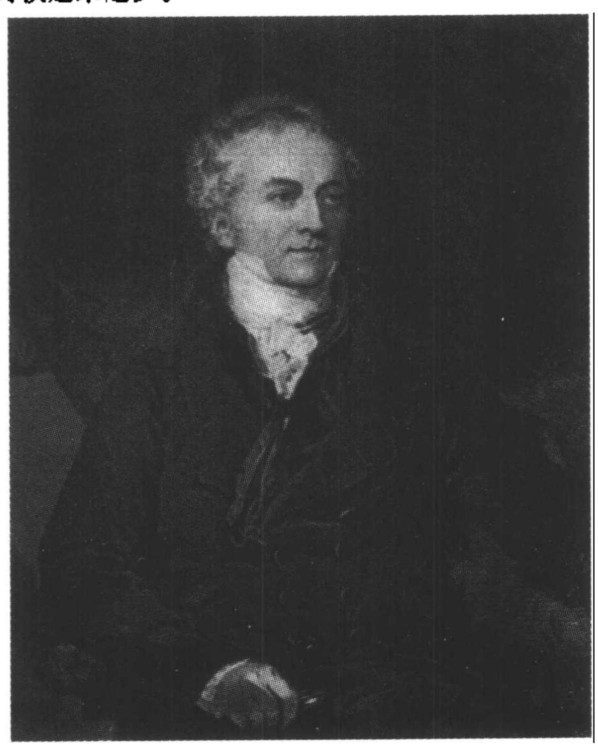


图 55:托马斯·杨

杨做了一系列非凡的医学实验，其中许多是来说明人的眼睛是如何工作的。他建立了眼睛如何分辨颜色的理论。他认为眼睛中有三种类型不同的受体，每一种对三原色之一都敏感。而对颜色的感知是三种受体共同作用的结果。通过把金属环箍在眼球上，他发现聚焦并不需要整个眼睛变形，所以，他推测内在的棱镜完成了聚焦的工作。他对光学的兴趣带着他走向物理学，并作出了又一系列的发现。他发表的论文《光的波动理论》是关于光的本质的经典之作。他还对潮汐作出了更好的新解释。他正式定义了能量的概念。而且他在"弹性"学科方面发表了几篇奠基性的论文。杨似乎能够解决任何学科的问题。但这对他来说并不能完全说是有利的。他的思维很容易被问题迷住，以至于他常常还没有解决完一个问题就跳到另一个新的问题上去了。

当杨听说了罗塞塔之石，它成为了杨无法拒绝的挑战。1814年的夏天，他去沃信海滨胜地度年假，这次，和他同行的还有一份罗塞塔碑文的复本。杨把注意力集中在被一个称为涡卷饰的圈包着的一串埃及象形文字上。他发现这就是突破点。他的直觉认为这些文字之所以被包起来，是因为它们代表的东西是非常重要的，比如说，法老托勒密的名字。因为，希腊文的碑文中也提到了法老托勒密的名字。如果是这样，杨就有可能从语音着手推测相对应的象形文字了，因为无论哪种语言中法老的名字的读音是一样的。托勒密涡卷饰在罗塞塔碑文中出现了六次，有时候以我们称为"标准"的形式出现，有时候以一种更长更精致的形式出现。杨假定长的形式是因为托勒密法老在名字前面加了头衔，所以他集中精力研究"标准"形式，猜测每个象形文字的读音(见表 13)。

杨当时并不知道他已经找到了大多数象形文字的正确读音。幸运的是，杨正确的判断了头两个象形文字(□,⌓)的语音顺序。它们看起来是一个叠在另一个的上面。之所以这样写象形文字完全是为了美感，可是，这样就牺牲了语音的明确性。雕刻倾向于写

成这样是为了避免间隙从而达到视觉上的和谐。有时,他们甚至在语音拼写较敏感的地方交换字母,反的方向拼写,纯粹为了加强雕刻文字的美感。做完这次破译,杨发现在塞柏的卡尔奈克神殿上也有带有涡卷饰的文字,他怀疑那是法老托勒密的皇后贝蕾尼卡的名字。他再次运用了他的破译方法,结果见表 14。

表 13:杨对罗塞塔之石上托勒密涡卷饰的译音与标准译音的对比表。

象形文字	杨的译音	标准译音
	p	p
	t	t
	optional	o
	lo or ole	l
	ma or m	m
	i	i or y
	osh or os	s

表 14:杨对卡尔奈克神殿上的贝蕾尼卡涡卷饰的译音与标准译音的对比表。

象形文字	杨的译音	标准译音
	bir	b
	e	r
	n	n
	i	i
	optional	k
	ke or ken	a
	feminine termination	feminine termination

在两个涡卷饰中有 11 个象形文字,杨完全正确地识别出其中的一半,还有 1/4 近乎正确。他还成功地辨别出表示女性名的后

缀。在皇后和女神后面都有这个后缀。虽然当时他不知道自己有多么成功，但在两个涡卷饰都出现的⺌都代表 i，这一点至少能给杨以信心，使他继续做他的破译工作。然而，他的工作突然搁浅，停滞不前了。可以看出，杨对基尔舍认为象形文字是表形符号的观点仍有太多的保留。他不打算破解这个范例。他对他语音上的发现是这样辩解的：托勒密王朝是亚历山大大帝的将军拉古斯的后裔，所以，托勒密实际上是外国人。杨猜想他们的名字之所以被拼出来是因为在象形文字中没有相对应的表形符号。他通过对象形文字与中文的进行对比总结了他的工作。那时，中文才刚刚为欧洲人所了解：

> 追溯象形文字中产生的字母式的书写，这是非常有趣的。这种现象在一定程度上可以用现代中国人拼写外来文的方式说明。字本身放弃了它的意思，而变成了简单的相似音的代表。这种现在印在书上的符号与带环的象形文字名字有许多相似之处。

杨把他的成就称为“休闲时几个小时的娱乐”。他对象形文字失去了兴趣，对他的工作作出结论后，他把他的工作总结成文，并发表在《1898 年大英百科全书增刊》上。

与此同时，法国的一个有前途的年轻的语言学家让·弗朗科依斯·钱普里昂正准备把杨的工作推到正确的结论上。虽然还不到 30 岁，钱普里昂已经对象形文字着迷了近 20 年。1800 年，法国数学家傅立叶让年仅 10 岁的钱普里昂参观了他收藏的古埃及遗物。他是拿破仑最早的“哈巴狗”之一。许多收藏上面都刻有奇怪的文字。傅立叶告诉这个孩子没有人懂得上面写的是什么。于是，这个孩子许下诺言，在将来的某一天他会解决这个谜题。从此，钱普里昂对象形文字着了迷。7 年后，在他 17 岁那年，他发表了一篇

名为《法老的埃及》的论文。这篇论文非常具有新意,他被推荐到格勒诺布尔学院工作。当钱普里昂听到他成了一个十来岁的教授时,他禁不住心中的喜悦,昏倒在地上。

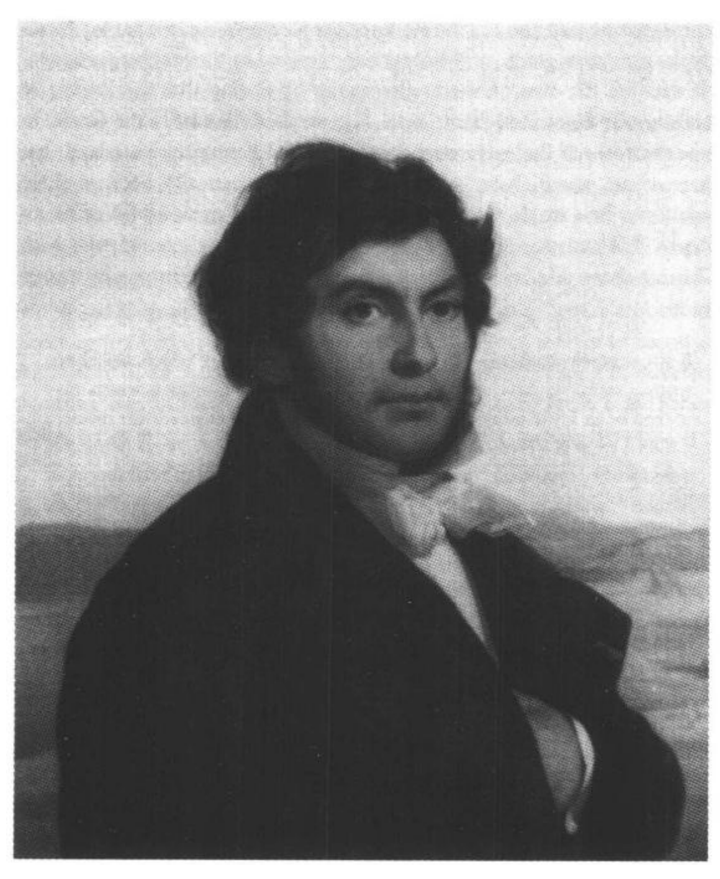


图 55:让·弗郎科依斯·钱普里昂

钱普里昂继续让他的同僚惊奇。他掌握了拉丁语、希腊语、希

伯来语、埃塞俄比亚语、梵语、古波斯语、钵罗钵语、阿拉伯语、叙利亚语、迦勒底语言、波斯语和汉语。而这一切都为他出击破译象形文字做好了充足的准备。发生在1808年的一个小故事说明了他的痴迷程度有多深。当时,他在街上碰到了一个老朋友。闲聊中这个朋友不经意提到一个著名的埃及学家亚历山大·莱诺尔出版了一本关于象形文字的完全破译的书。钱普里昂是如此的沮丧,他整个人当场就昏倒在地上(他似乎很有晕倒的天赋)。他活着的整个理由看起来就是为了第一个阅读古埃及的文字。幸运的是,莱诺贝的破译几乎和基尔舍在17世纪所做的尝试一样荒诞不羁。挑战仍然存在。

1822年,钱普里昂试着把杨的方法运用到其他的涡卷饰上。英国博物学者W·J·班克斯带着一座刻有希腊文和象形文字的方尖石塔到了多塞特,并且不久后出版了这两个文字的石版画。其中就有托勒密和克娄巴特拉的涡卷饰。钱普里昂得到了一份复本,而且把象形文字与它们的读音联系起来(表15)。字母p,t,o,l和e在两个名字中都有,其中4个在托勒密和克娄巴特拉中代表它们的象形文字是相同的。只有一个t有差别。钱普里昂推测t的音可能被两个象形文字表示,就像英语中[k]的音可以用c或k来表示。比如,cat(猫)和kid(小孩)中的c和k都发[k]的音。在成功的希望里,钱普里昂开始试着破译一些没有双语翻译的涡卷饰。他从托勒密和克娄巴特拉涡卷饰上推出的一批象形文字的读音,并以此为标准,尝试推出其他涡卷饰的读音。他的第一个神秘的涡卷饰(见表16)中藏着一个古代伟大人物的名字。钱普里昂很容易看出来,这个看起来很像a-l-? -s-e-? -t-r-? 的涡卷饰代表名字alksentrs(希腊文中拼作Alexandros,英文中拼作Aleaxander,也就是亚历山大)。而且他还可以看到这文字中并不爱使用元音,常常省略掉它们;这种文字假设读者可以不费劲地自己添上缺失的元音。又有了两个象形文字的经验,这位年轻的学

者研究了其他的碑文并且破译了一系列的涡卷饰。不管怎样，这一切仅仅是杨的工作的继续。所有的这些名字，包括亚历山大和克娄巴特拉，仍然都是外来名。杨仅有的外来名是拼出来的理论，仍能够解释这一切。

表 15：钱普里昂对方尖石塔上托勒密涡卷饰 和克娄巴特拉涡卷饰 的破译。

象形文字	音标
	p
	t
	o
	l
	m
	e
	s

象形文字	音标
	c
	l
	e
	o
	p
	a
	t
	r
	a

表 16：钱普里昂对亚历山大涡卷饰 的破译。

象形文字	音标
	a
	l
	?
	s
	e
	?
	t
	r
	?

在1822年9月14日，钱普里昂得到了一些阿布辛贝神殿的浮雕品。其中含有可以追溯至格雷克－罗曼统治时期的涡卷饰。这些涡卷饰有着不同寻常的意义。它们非常古老，所以其中有着传统的古埃及名字，而且它们也是拼出来的。这个证据彻底推翻了仅有外来名是拼出来的理论。钱普里昂将注意力集中在了一个仅仅含有四个象形文字的涡卷饰上：前两个象形文字是未知的。但后两个重复的文字可以从亚历山大(Alksentrs)涡卷饰中得知，它们都代表s。这意味着这个涡卷饰代表(？－？－s－s)。此刻，钱普里昂运用上了他广博的语言学知识。虽然从埃及古语发展出来的科普特语在11世纪已经不再作为一种生活用语使用了，但是，在基督教科普特教堂中的礼拜仪式中，科普特语仍然以非常古老的形式使用着。钱普里昂十几岁时学过科普特语，他甚至可以用科普特语记录日志。然而，在此刻之前，他从没有想到科普特语也是一种'象形文字'的语言。

这个涡卷饰的第一个文字☉很像是一幅太阳的图画。钱普里昂怀疑它是一个表意符号，代表词可能是太阳。然后，天才般的直觉让他认为这个表意符号的读音应该是科普特语中太阳的读音ra。这样序列就变成了(ra－？－s－s)。只有一个法老的名字可能满足。在准许元音被省略的情况下，假设未知的文字代表m。那么这肯定是最伟大、最古老的法老之一拉梅西斯的名字。破译出了这个拼写，说明即使古老的传统的古埃及名字也是按音拼写出来的。钱普里昂冲进他兄弟的办公室，宣布："Je tiens l'affaire!"(我找到了！)然而，当钱普里昂对象形文字的无限痴迷得到回报时，他突然又昏倒了，后来的5天，他不得不在病床上度过。

钱普里昂破译这些文字有时采用了"字谜"游戏的规则。在字谜游戏中，长的单词被分成几个音节，每个音节由一个表意符号表示。这种现象在现在的孩子游戏中仍能见到。比如说，单词belief(信念)可以分成两个音节bee(蜜蜂)和leaf(树叶)。除了用字母

表示出来,它还可以表示成一个蜜蜂的图画紧接上一片树叶的图画。在钱普里昂发现的例子中,只有第一个文字(ra)太阳的图画是由一个"字谜"规则的图画表示的。而剩下的文字是按照传统习惯拼写的。

在拉梅西斯涡卷饰中的太阳这个表意符号的意义重大。因为它明显地限制了抄录员所说的语言的可能。比如说,抄录员不可能说希腊语,因为如果是那样,这个涡卷饰就会读成"helios - meses"。涡卷饰只有用一种形式的科普特语读出,才有意义,因为只有这样涡卷饰才会读成"ra - meses"。

虽说只多了这么一个涡卷饰,它的破译却说明了象形文字的四条原则。第一,文字的语言至少与科普特语有联系。事实上,对其他象形文字的检验表明它就是纯正简单的科普特语。第二,表意符号用来表示某些单词,比如,"太阳"就是有一个形似太阳的符号表示的。第三,长的单词可以全部或部分通过"字谜游戏"规则拼出。最后,古代抄录员依赖一种传统的发音字母表示方式拼写出了大多数的文字。最后的一点是最关键的一点。钱普里昂称语音学是象形文字的"灵魂"。

运用他深厚的科普特语言的知识,钱普里昂开始毫无障碍的对大量的象形文字进行破译。他的工作远远超出了涡卷饰的范围。不到两年,他识别了大多数象形文字的读音。他还发现其中某些象形文字代表两个甚或三个辅音的组合。这使得抄录员既可以选用一些简单的象形文字拼写一个单词,也可以选用几个"多辅音"象形文字拼写。

钱普里昂把他的初步结果邮寄给了法国铭文科学院秘书达西耶先生。然后,在 1824 年,钱普里昂 34 岁那年,他在一本书中发表了他全部成就。14 个世纪来,第一次有可能阅读法老的抄录员所记录的法老的历史。对于语言学家,这是一个契机,他们可以去研究跨越了 3000 年的语言和文字的进化。象形文字的历史可以

追溯到公元前 300 万年，一直到公元 4 世纪。不仅如此，象形文字的演化可以与僧侣书写体和现代希腊语文字相类比。它们现在也被破译了。

几年中，因为政治上的原因和别人的忌妒，钱普里昂的非凡成就一直没有被广泛承认。托马斯·杨尤其是一个刻薄的批评者。在某些场合，杨否认象形文字可以广泛的表语音；而在其他时候他又接受了这个观点，但是抱怨自己比钱普里昂更早地得出这个结论，而那个法国人无非是填补了一些漏洞而已。杨的敌意大多数是因为钱普里昂不分给他任何的功劳，即便非常可能是杨的工作启发了整个破译工作。

1828 年 7 月，钱普里昂开始了他的第一次埃及之旅。这次旅行为期 18 个月，这对他来说是个绝佳的机会。他可以亲眼目睹真正的碑文了，而以前他只能看到碑文的图画和平版画。30 年前，拿破仑的探险队只能胡乱地猜测装饰神殿的象形文字的意思，而现在，钱普里昂可以逐字逐名地读出它们而且重新正确地解释它们。他的拜访是及时的。三年后，他完成了他的埃及之行所有的笔记、图画和翻译。之后，他就一病不起。伴随着他一生的一次次昏倒看起来就是严重病症的征兆。他强迫性的高强度工作使病情恶化。他死于 1832 年 3 月 4 日，年仅 41 岁。

B 类楔形文字之谜

在钱普里昂的突破之后的两个世纪，古埃及学研究者继续提高他们对复杂的象形文字的理解。他们的理解水平达到了相当高的程度，他们甚至可以破解加密的象形文字。这种象形文字可能是世界上最古老的密文了。一些在法老的陵墓中所发现的碑铭被加过密，加密方法也不尽相同，其中包括替换加密法。有时，生造

的符号会替代原有的象形文字，而另一些时候，音不同但形相似的象形文字会替代掉正确的文字。比如说，代表 f 的“长角的蛇”会替代代表 z 的“大毒蛇”。通常，这种加密并不像是难已破解的，而更像是给过路人出的谜题，让他们在陵墓旁逗留更长的时间。

征服了象形文字后，考古学家继续破译了许多其他的古老文字，其中包括巴比伦的楔形文字，土耳其的 Kök – Turki 的神秘文字，印度的布兰姆字母表。然而，对于正在成长中的钱普里昂们仍有几个未解的谜题在等着他们。比如说伊特鲁里亚和印第安文字。破译这些文字的巨大困难是没有任何双文对照。没有了它，密码破解者对古代文字的内容一无所知。在破译古埃及象形文字中，是涡卷饰充当了双文对照的角色，使杨和钱普里昂初尝语音破译的甜头。没有双文对照，古代文字的破译工作几乎是毫无希望的，但是，仍然有一个著名的事例说明破译古代文字也可以不需要双文对照的帮助。B 类楔形文字是一种可以追溯到青铜时代的克里特文字，在没有任何古代抄录员留下的双文对照的线索帮助下，被成功地破译了。它的破译完全是逻辑和灵感结合的结晶，也是一个纯密码破译的典型事例。事实上，B 类楔形文字的破译被广泛认为是所有考古破译中最为出色的一个。

B 类楔形文字的故事开始于亚瑟·埃文斯爵士的挖掘工作。他是世纪之交最著名的考古学家之一。埃文斯对荷马史诗《伊利亚特》和《奥德赛》所描述那段希腊历史非常感兴趣。荷马讲述了特洛伊战争的历史，即希腊人在特洛伊的胜利以及胜利后希腊英雄奥德赛的遭遇。据推测这些事情应该发生在公元前 12 世纪。一些 19 世纪的学者认为荷马史诗只是神话传说而已，但在 1872 年德国考古学家海恩里希·谢来曼发现了特洛伊的地点就在土耳其的西海岸附近时，出人意料地，荷马史诗从神话变成了历史。在 1872 年到 1900 年期间，考古学家发现了古希腊前海伦时期历史的进一步证据，这个时期比毕达哥拉斯、柏拉图和亚理士多德的时

期还要早 600 多年。前海伦时期的具体时间是公元前 2800 年到公元前 1100 年。在最后的 400 年间,这个文明达到了它自身的顶点。在希腊本土,它的中心是迈锡尼。在那儿,考古学家发现了大量的手工艺品和财宝。然而,使亚瑟·埃文斯爵士甚感困惑的是考古学家没有发现任何形式的文字。他不能接受如此复杂的文明竟然不会读写,所以,他决定证明迈锡尼文明是有文字的。

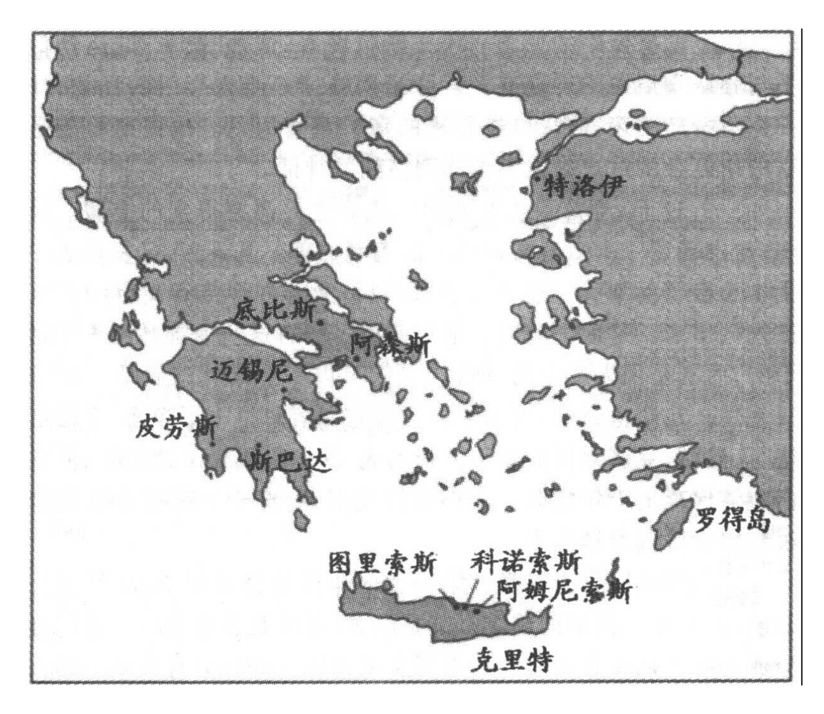


图 57:在古老的爱琴海的周围。在希腊本土上的迈锡尼有未开发的财宝,阿萨·尹万斯先生去寻找雕刻的碑石。第一个 B 类楔形文字的石碑就是在克里特岛上发现的。

亚瑟爵士和不同类型的雅典古玩商贩打过交道后,终于找到

了一些前海伦时期刻有文字图案的石头。这些图案看起来却更像是标记,和文章中用的符号相似,并非真正的书写文字。然而,这个发现使他动力十足,并继续他的追寻。据说这些标记来自于克里特岛的克诺索斯城,传说迈诺斯国王的宫殿就在这个地方,也是当时统治爱琴海的帝国中心。1900 年 3 月,亚瑟爵士动身去往克里特岛,开始了挖掘工作。挖掘的工作进行得很快,成果也是非凡的。他发现了豪华宫殿的遗迹,里面有复杂的过道,并且装饰有年轻人跳上愤怒公牛的壁画。埃文斯猜度着,这种"跳牛"的运动似乎与弥诺陶洛斯的传说有关。弥诺陶洛斯是半人半牛的怪物,住在克里特岛的迷宫内,以进贡来的童男童女为食。他提出可能是宫殿中复杂的过道启发了弥诺陶洛斯的神话。

3 月 31 日,亚瑟爵士开始边挖边寻他最渴望得到的宝藏。最初,他发现了一个带有文字图案的陶制的碑。几天后,又发现了一个木头箱子上刻满了这种文字。然后,又有许多带有文字的古玩被挖掘出来。这远远超出了他的期望。所有这些碑都是用太阳晒干的,而不是用火烘干的,所以,它们可以一沾水就溶解掉而被重复使用。几个世纪来,雨水早应该把它们溶解得干干净净,不留痕迹了,然而,克诺索斯城毁于一场大火,这场火烘烤了这些碑,使它们能够保存上千年之久。它们完好无损,以至于上面抄录员的指纹都依稀可以分辨出来。

这些碑可以分为三类。第一类的年代是公元前 2000 年到公元前 1650 年。其中的碑文全部是图画,可能是表意符号。很明显与亚瑟爵士从希腊古玩商那里买来的古玩上的标记有关系。第二类的年代是公元前 1750 年到公元前 1450 年,它上面的字符都是由简单的线组成,因此这种文字被命名为 A 类楔形文字,第三类的年代是公元前 1450 年到公元前 1375 年,上面刻的文字很像是精炼后的 A 类楔形文字。所以被命名为 B 类楔形文字。又因为它是最近的文字,亚瑟爵士和其他考古学家认为破译 B 类楔形文

字的可能性最大。

许多碑文中似乎含有详细的记载。有着这么多一行又一行的字符,数出字符种类的多少是相对比较容易的事。然而,要确定字符的读音是较为困难的事。它们看起来像是一些不含有任何意思的随意的涂鸦。历史学家大卫·卡恩是这么形容这些字符的:“哥特式的弧围绕着一条竖线,梯子,心里有一竖穿过它,带着钩的弯曲的三角叉,三条腿的恐龙向后看,A 字加上穿过它的一横,反方向的 S,半满的高啤酒杯加上在它边缘有一个弓形,还有许多的什么都不像。”关于 B 类楔形文字,只知道两个有用的事实。第一,书写的方向是由左至右的,因为行末的空白都出现在右侧;第二,总共有 90 个不同的字符。这暗示这种文字几乎肯定是音节式的,纯字母表式的文字大概多在 20 到 40 个字符之间(比如,俄语 36 个字母,阿拉伯语 28 个字母)。而另一个极端,基于表意符号的文字往往含有成百上千个字符(汉语的文字就超过 5000 个)。音节式的文字在它们的中间,一般有 50 到 100 个字符。除了以上两点,B 类楔形文字是一个深不可测的谜。

基本的问题是没有人能确定 B 类楔形文字书写的是哪一种语言。最初,有人推测 B 类楔形文字是希腊语的一种书写方式,理由是 7 个符号很像塞浦路斯希腊语的文字,这种希腊文字曾在公元前 600 年到公元前 200 年间使用。但是,疑义开始出现了。希腊单词常常以辅音 s 结尾,因此,在塞浦路斯希腊语中词的结尾常常是ᚩ。它表示音节 se,因为一个字符是表示一个音节的,单独的辅音则用辅音和元音复合体来表示,但元音不发音。同样的字符也出现在 B 类楔形文字中,但它却很少在词尾出现,这表示 B 类楔形文字不可能是希腊文。大多数的意见认为 B 类楔形文字书写的是一种已经消失的语言,当这种语言消失后,它的文字保留下来,并经过几个世纪后,逐渐演化成了塞浦路斯希腊语文字。因此虽然两种文字很相像,但它们所代表的是完全不一样的两种语言。



图 58：一块 B 类楔形文字石碑，约公元前 1400 年。

亚瑟·埃文斯爵士是B类楔形文字并非希腊文的理论的重要支持者。他相信B类楔形文字代表的是一种克立特当地的语言。他的很多考古证据能做为他观点的佐证。比如,他在克立特岛上的发现表明,迈诺斯国王的帝国,也就是迈诺斯帝国,远远比地中海的文明大陆更为先进。迈诺斯帝国不是迈锡尼帝国的附属,而是一个对手,甚至是它的主宰。弥诺陶洛斯的神话说明了这两个文明当时的地位。这个传说描述了当时迈诺斯国王要求雅典献上年轻男女,来作为迈诺陶洛斯的牺牲。简言之,埃文斯做出的结论认为既然迈诺斯帝国如此强大,它应该保留着自己的语言,而不会用它对手的语言——希腊语。

虽然,大多数人接受了迈诺斯人说的是自己的语言(B类楔形文字是这种语言的一种文字),而非希腊语,仍然有一两个异端者争辩道弥诺斯人说和写的都是希腊文,亚瑟爵士并没有从轻处罚这些持不同意见者,他利用他的影响力严惩了这些人。剑桥大学的考古学教授A·J·B·维斯放言说B类楔形文字可能代表希腊文。亚瑟爵士把他逐出了所有的挖掘工作,并且强迫他退出了雅典的一所英国学校。

1939年,"希腊文与非希腊文"之争论逐渐升温,因为辛辛那提大学的教授卡尔·波里根在皮劳斯的涅斯托尔宫殿中也发现了刻有B类楔形文字的碑。这是不同寻常的,因为皮劳斯地处希腊大陆,曾是迈锡尼帝国而非弥诺斯帝国的领土。少数认为B类楔形文字是希腊文的考古学家认为这个发现支持了他们的假说:B类楔形文字在说希腊语的大陆上发现,所以,它代表的是希腊语;B类楔形文字也在克立特岛上发现,所以,迈诺斯人也说希腊语。而埃文斯阵营的考古学家们用同样的方式论证了完全相反的观点:克里特岛上的迈诺斯人说迈诺斯语;在克立特岛上发现了B类楔形文字,所以B类楔形文字代表迈诺斯语;在希腊大陆上也发现了B类楔形文字,所以,希腊大陆上的人也说迈诺斯语。亚

瑟爵士武断地认为："在迈锡尼没有说希腊语的王朝的容身之地……这个文明和语言一样，是以迈诺斯为主的。"

事实上，波里根的发现并不需要把同一种语言强加给迈锡尼和迈诺斯。在中世纪，许多欧洲国家，不管它们的本国语言是什么，都使用拉丁文来作记录。B 类楔形文字这种语言可能就是爱琴海周围商贩的一种通用语言，它使不同母语国家的交易变得容易。40 年来，所有破译 B 类楔形文字的努力都以失败而告终。1941 年，亚瑟爵士逝世，时年 91 岁。他没有活到目睹 B 类楔形文字被破译的那一天，也没法亲自阅读他发现的碑文的意思。实际上，在此刻，破译 B 类楔形文字的前景一片黯淡。

连接的音节

亚瑟·埃文斯爵士逝世之后，他发现的碑和考古笔记被严格地限定在一圈支持他的观点的考古学家中。他们坚信 B 类楔形文字是一种失传的迈诺斯语的文字。然而，在 20 世纪 40 年代中期，一位布鲁克林大学的考古学者艾丽丝·科伯设法取得了这些资料，并且开始仔细而又无偏颇的分析这种文字。对于跟科伯只有一面之交的人来说，科伯显得非常的普通——一个寒酸的教授，既不迷人，也没有性格，生活上简单朴素。但是，她的研究热情是不可估量的。伊娃·布兰是科伯的学生，她去了耶鲁大学并成了一名考古学家，她是这么回忆她的老师科伯的："她以一种刚柔相济的方式工作着。她曾经告诉我如果要知道自己什么时候做了一件真正伟大的工作，惟一途径是那时你的脊椎有刺痛的感觉。"

为了破译 B 类楔形文字，科伯知道她必须抛弃所有的成见。她把注意力只放在全部文字的结构和单独词汇的构造上。她特别注意到一些单词按其形式可以三个一组归类，每一组词像是同一

个词的三种形式。在同一组的三个词中，主干是相同的，而有三种不同的词尾。她得出的结论是 B 类楔形文字是一种词形变化高度发达的文字，就是说词尾的变化反映了词性、时态、主格还是宾格等等。英语也有一些词形变化。比如说，我们讲"I decipher（我解码），you decipher（你解码），he deciphers（他解码）"——在第三人称作主语时，动词后面加了 s。



图 59：艾丽丝·科伯

使用这种古老的语言倾向于更严格更极端的词形变化。科伯发表了一篇论文陈述了两组词的词形变化的性质（见表 17）。每组词的主干都是一样的，但根据三种不同的形式有着三种不同的

词尾。

表 17:B 类楔形文字中的两组相变化的词

	单词1	单词2
形式1	[illegible]	[illegible]
形式2	[illegible]	[illegible]
形式3	[illegible]	[illegible]

为了方便讨论,每一个 B 类楔形文字的符号用一个二位数代替。见表 18。利用这种替代法,表 17 中的文字可以重新改写成表 19 中的样子。两组词可能都是名词,根据不同的格有着不同的词尾,比如说可能形式 1 是主格,形式 2 是宾格,形式 3 是与格。很明显的是,两组词的前两个符号(25 - 67 - 和 70 - 52 -)都是主干。因为它们不随格的变化而变化。可是,第三个符号就有点让人迷惑了。如果第三个符号属于主干,那么它应该保持不变,不管是什么形式,但事实并非如此。在词 A 中,第三个符号在形式 1 和形式 2 中是 37,在形式 3 中却是 12。在词 B 中,第三个符号在形式 1 和形式 2 中是 41,在形式 3 中是 12。相反的,假设第三个符号属于词尾而不属于主干。这种同样的问题仍存在着。一个特定的形式的词尾应该是固定的,不管单词主干是什么。但在形式 1 和形式 2 中,词 A 的第三个字符是 37,词 B 则是 41。在形式 3 中,词 A 的第三个符号是 05,而词 B 的却是 12。

表 18:与 B 类楔形文字符号相对应的二位数

01		30		59	
02		31		60	
03		32		61	
04		33		62	
05		34		63	
06		35		64	
07		36		65	
08		37		66	
09		38		67	
10		39		68	
11		40		69	
12		41		70	
13		42		71	
14		43		72	
15		44		73	
16		45		74	
17		46		75	
18		47		76	
19		48		77	
20		49		78	
21		50		79	
22		51		80	
23		52		81	
24		53		82	
25		54		83	
26		55		84	
27		56		85	
28		57		86	
29		58		87	

表 19:两组以数字写成的 B 类楔形文字符号

	单词1	单词2
形式1	25-67-37-57	70-52-41-57
形式2	25-67-37-36	70-52-41-36
形式3	25-67-05	70-52-12

第三个符号不符合预想，因为它既不像是主干，又不像是词尾。科伯解决了这个矛盾，她建立了一套理论认为每个符号代表的是一个音节，假设每个音节是由一个辅音和一个元音共同构成。她提议第三个音节是一个连接音节。它的辅音来自于主干，而元音却是词尾的一部分。为了说明她的理论，她举了一个阿卡得语的例子。阿卡得语是一个具有词形变化的语言，而且有连接音节。一个阿卡得语名词在形式 1 中是 sadanu，在形式 2 中变化成了 sadani，而在形式 3 中则是如表 sadu。如表 20 很明显，三种形式都含有主干 sad - ，而词尾分别是 - anu(形式 1)，- ani(形式 2)， - u(形式 3)，那么 - da - ，- da - 和 - du - 就分别是它们的连接音节了。连接音节在形式 1 和形式 2 中是相同的，而在形式 3 中是不同的。这和 B 类楔形文字中所观察到的模式一模一样。B 类楔形文字单词的第三个符号一定是一种连接音节。

表 20:连接音节在阿卡得语中发 Sadanu 的音

形式1	sa-da-nu
形式2	sa-da-ni
形式3	sa-du

光是发现 B 类楔形文字的词形可变性和连接音节的存在，就意味着科伯已经远远走在其他破译者的前面了。但这只是个开

始。她正要作出更重要的推测。在阿卡得语的例子中,连接音节从 - da - 变成 - du - ,但是辅音在这两个音节中是一样的。类似的,B 类楔形文字的字 37 和 05(在词 A 中),必定有着同样的辅音。而词 B 中的字 41 和 12 共享一个辅音。自从埃文斯发现 B 类楔形文字以来,第一次关于这文字的语音的事实开始呈现出来。科伯还可以建立这些文字的其他的关联。很明显,词 A 和词 B 在形式 1 中有着相同的词尾。然而,连接音节却分别是 37 和 41。这意味着符号 37 和 41 有着不同的辅音和相同的元音。这样可以解释这两个词为什么符号不一样,却有着相同的词尾。对形式 3 作相似的推论,可以知道字 05 和 12 也有着不同的辅音和相同的元音。

科伯并不能指出字 05 和 12,或者字 37 和 41,究竟共享的是哪一个元音。同样,她也无法指出字 37 和 05,或者字 41 和 12,共享的是哪一个辅音。然而,在不考虑它们的具体读音的情况下,她建立了一套这些文字的严格关系。她用表格的形式总结了她的初步结果(见表 21)。这一切是说,即使她不知道字 37 究竟读什么音,但她知道它的辅音和字 05 相同,而元音和字 41 相同。类似的,她不知道字 12 读什么音,但她知道它的辅音和字 41 相同,而元音和字 05 相同。她把她的方法运用到其他单词上,从而最终建立了包含 10 个字符的关系表。这张表宽有两个元音,长有五个辅音。科伯很可能会尝试做进一步的工作,也很有可能最终能够破译整个文字,但她于 1950 年因肺癌去世了,年仅 43 岁。

表 21:科伯最初的 B 类楔形文字特点表格

	元音 1	元音 2
辅音 I	37	05
辅音 II	41	12

琐碎的枝节

在艾丽丝·科伯去世前几个星期,她收到了一封来信,发信人是迈克尔·文特里斯,一位英国的建筑师。他从小就对B类楔形文字着了迷。文特里斯出生于1922年7月12日,他的父亲是一名英国军官,母亲有一半的波兰血统。他对考古的兴趣源自于他母亲的鼓励,她常常带他去参观大英博物馆,他被古代世界的奇迹深深吸引着。迈克尔是个聪明的孩子,而且有着惊人的语言天赋。他小学是在瑞士的格施塔德上的,在那儿,他的法语和德语逐渐流利起来,而且在6岁的时候,他开始自学波兰语。

和让·弗郎科依斯·钱普里昂一样,文特里斯从小就对古代文字着了迷。7岁那年,他读了一半关于古埃及象形文字的书。对于这么小的孩子来说,这已经是一项不小的成就了,更不用说,这本书是用德文写的。对古代文明的文字的兴趣伴随着他的整个童年。14岁时,他听了B类楔形文字的发现人亚瑟·埃文斯爵士的讲座,他的兴趣就更加浓厚了。年轻的文特里斯听说了迈诺斯文明和B类楔形文字后,暗下决心要破译这种文字。从那天起,他对B类楔形文字的痴迷陪伴着他走过了他短暂而又辉煌的一生。

18岁的时候,他把他对B类楔形文字最初的想法总结成文,并发表在非常有权威性的期刊《美国考古学期刊(American Journal of Archaeology)》上。当他提交这篇论文时,他有意回避了他的年龄,生怕编辑不严肃对待他的论文。他的论文十分支持亚瑟爵士的观点,批评了B类楔形文字是希腊语的假说,他是这么陈述的:"认为迈诺斯语是希腊语的理论显然是基于一种故意忽视历史的狡辩。"他个人的观点是认为B类楔形文字来自于伊特鲁里亚语。一个有说服力的理由是有证据表明伊特鲁里亚人曾在爱琴海

居住，之后才定居意大利。虽然他在论文中并没有尝试破译 B 类楔形文字，但他非常肯定地写道："它是可以破译的。"

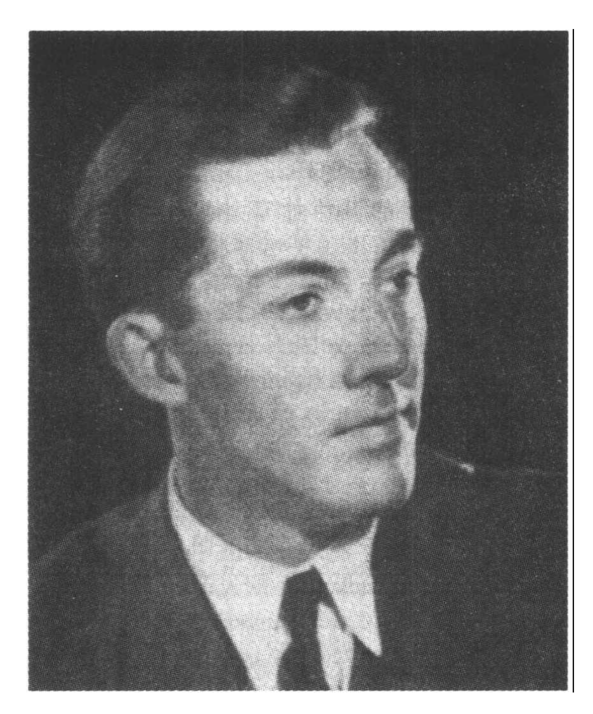


图 59：迈克尔·文特里斯

文特里斯成为了一名建筑师，而非职业考古学家，但他仍保留着对 B 类楔形文字的浓厚兴趣。他所有的业余时间都花在研究这种文字上了。当他听说了艾丽丝·科伯的工作后，他渴望得知她的突破，因此，他写信给她询问更详细的细节。虽然她没来得及回信就去世了，然而她的想法可以在她的出版物中找到，文特里斯仔细地研究了它们。他完全意识到了科伯表格的威力，于是，他尝试

着寻找更多的共享主干并且有连接音节的词,从而扩展了科伯的表格,加入了许多其他的辅音和元音。经过多年的研究,他发现一个特别的现象——似乎有证据表明并非所有的B类楔形文字符号都是表示音节的。

大多数人都同意一个B类楔形文字符号表示一个辅音和一个元音的组合[①],因此,拼写一个单词需将它分解成若干个CV组合。比如说,英文单词 minute(分)就拼成 mi - nu - te,三个CV组合的符号。但是,并不是所有的单词都可以很方便的分成CV组合的。比如说,如果我们把单词"visible"(可见)分解成两个字母一对,我们得到的是"vi - si - bl - e",这就出现了问题,它并不是一系列的简单的CV组合。其中有一对双辅音符号和一个单独的 - e 在词尾。文特里斯假设弥诺斯人通过在词中加入不发音的 i 克服了这个困难,这个词可以被写成 vi - si - bi - le ,又可以表示成一系列的CV组合了。

然而,拼写单词"invisible"(不可见)仍然存在着问题。我们又一次需要加上不发音的元音,这次是在 n 和 b 后面,使它们能够表示成CV符号。不仅如此,还需要处理一下 i - ni - vi - si - bi - le 词首的单个元音 i ,词首的 i 不容易变成CV结构,因为在词首加上不发音的辅音很容易造成混淆。总之,文特里斯的结论是B类楔形文字中有表示单个元音的符号。这些符号是容易辨认出来的,因为它们只出现在词首。文特里斯研究了符号出现在词首、词中和词尾的频率。他观察到两个特别的符号08和61,绝大多数出现在词首。他下结论道,这两个符号代表元音,而非音节。

文特里斯以一系列的工作笔记的形式发表了他的元音符号的想法和他扩展的表格,从而使其他的B类楔形文字研究者了解他的工作。1952年6月1日,他发表了他最有意义的结果——工作

① 辅音的英文是 consonant,元音的英文是 vowel,因此辅音和元音记做CV。——译者注

表 22:文特里斯的表示 B 类楔形文字符号之间关系的扩展表格。虽然表格中没有指定元音或辅音,但却显示了哪几个符号有共同的辅音和元音。比如说,所以在第一栏里的符号有相同的元音,则标作 1。

		元音字母				
		1	2	3	4	5
辅音	I					57
	II	40		75		54
	III	39				03
	IV		36			
	V		14			01
	VI	37	05		69	
	VII	41	12			31
	VIII	30	52	24	55	06
	IX	73	15			80
	X		70	44		
	XI	53				76
	XII		02	27		
	XIII					
	XIV			13		
	XV		32	78		
	纯元音		61			08

笔记 20,这成为破译 B 类楔形文字的转折点。他花了两年的时间扩展科伯的表格,他的结果如表 22 中所示。这个表格含有 5 个元音列和 15 个辅音行,总共有 75 个格子,再加上 5 个表示单元音的格子。文特里斯填了大约有一半的样子。这个表格是信息的宝藏。比如说,第六行就告诉我们符号 37,05 和 69 有着共同的辅音 IV,但是有不同的元音 1,2 和 4。文特里斯并不知道辅音 IV 和元音 1,2,4 的具体读音,到此刻,他抵抗住了给符号赋予读音的诱惑。然而,他觉得是该跟着感觉猜几个读音并检验结果的时候了。

文特里斯注意到三个单词不断地在 B 类楔形文字碑文中出

现:08－73－30－12,70－52－12 和 69－53－12。仅仅出于直觉的考虑,他猜测这三个单词是三个重要城市的名称。文特里斯已经推断出 08 代表一个元音。而惟一能符合这个单词的重要城市是港口城市阿姆尼索斯。如果他是正确的,那么第二个和第三个符号 73 和 30 就分别代表－mi－和－ni－。这两个符号有着共同的元音 i,所以 73 和 30 应该在同一个元音列出现,它们确实是这样。最后一个符号 12 代表－so－,而没有符号可以代表词尾的 s。文特里斯决定暂时忽略没有词尾 s 的问题,他实施了以下的翻译:

城市 1 ＝ 08－73－30－12 ＝ a－mi－ni－so ＝ Amnisos

这只是一个猜测,但将它运用到文特里斯的表格上,它的作用是巨大的。比如,符号 12 看起来是代表－so－,在第二个元音列和第七个辅音行上。因此,如果这个猜测是正确的,那么所有在第二个元音列上的符号都含有元音,而所有在第七个辅音行都含有辅音 s。当文特里斯检查第二个城市时,他注意到了它也含有符号 12,－so－,另两个符号是 70 和 52,它们和－so－在同一列。这意味着这两个符号都含有元音 o。他把－so－,o 填到了它们的位置,留下未知的辅音。如下:

城市 2 ＝ 70－52－12 ＝ ？o－？o－so ＝ ？

这可能是克诺索斯吗? 这些符号表示 ko－no－so。又一次,文特里斯很高兴地忽略了没有词尾 s 的问题,至少,这是暂时的。他非常愉快地看到符号 52 代表－no－,和符号 30 在阿姆尼索斯中代表－ni－,是在同一辅音行中。这又验证了他的猜测,因为,如果它们都含有同一个辅音 n,那么它们的的确确是应该在同一辅音行中。利用从克诺索斯和阿姆尼索斯中得到的信息,他把第三个城市添上了以下的字母:

城市 3 ＝ 69－53－12 ＝ ?? －？i－so

惟一符合的名字看起来是图利索斯(tu－li－so),是一个克里特中部的重要城市。再一次,词尾的 s 消失了,而文特里斯又一次

忽略了这个问题。他试验性地识别了 3 个地名，和 8 个不同符号的读音：

城市 1 = 08 - 73 - 30 - 12 = a - mi - ni - so = Amnisos

城市 2 = 70 - 52 - 12 = ko - no - so = Knossos

城市 3 = 69 - 53 - 12 = tu - li - so = Tulissos

识别 8 个符号读音的影响是巨大的。文特里斯可以通过表格推出许多其他符号的读音(如果它们是在同一行或同一列)。结果是，得知了许多符号的一半读音和一些符号的全部读音。比如说，符号 05 和符号 12(so)，52(no)，70(ko)在同一列，所以它一定含有元音 o。同样的道理，符号 05 和符号 69(tu)在同一行，所以，它的辅音一定是 t。综上所述，符号 05 代表音节 - to - 。再看看符号 31，它和符号 08(元音 a)同一列，和符号 12(辅音 s)同一行，所以，符号 31 代表音节 - sa - 。

推断出 05 和 31 的读音是异常重要的，因为这样就使文特里斯能够读出两个完整单词的读音了。05 - 12 和 05 - 31，这两个词常常出现在记载目录的结尾处。文特里斯已经知道符号 12 代表音节 - so - ，因为这个符号出现在词 Tulissos 中，因此 05 - 12 可以读成 to - so。而另一个词 05 - 31 可以读成 tu - sa。这是个惊人的结果。因为专家曾猜测这些在记载目录结尾处的词的意思是“全部”。文特里斯现在把它们读成 toso 和 tosa，与古希腊语 tossos 和 tossa 有惊人的相似。分别是词组“so much”(意思是：就这么多了)的阳性和阴性格式。自打他 14 岁时听到亚瑟·埃文斯爵士的讲演起，他始终相信迈诺斯的语言不可能是希腊语。现在，他揭示的单词读音却成了 B 类楔形文字是希腊语的有力证据。

塞浦路斯希腊语文字最初被认为是 B 类楔形文字而不是希腊语。因为 B 类楔形文字中的单词很少以 s 结尾的，而希腊语中最常用的词尾就是 s。文特里斯发现 B 类楔形文字确实是很少用 s 结尾，但这可能仅仅是因为由于书写的习惯 s 被省略掉了。Am-

nisos, Knossos, Tullissos 和 tossos 的拼写都缺少了词尾的 s,这意味着 B 类楔形文字的书写根本不考虑词尾的 s,而是由读者在阅读时自己加上这明显忽略的 s。

文特里斯很快就破译了一些其他的单词,而且它们也很像希腊的词汇,可是,他还不能完全确信 B 类楔形文字就是希腊语的文字。从理论上来讲,他所破译的单词都可以看作迈诺斯语的外来语。外国人来到英国旅馆,可能会无意中听到像"rendezvous(约会)"或者"bon appetit(祝好胃口)"这样的词,但只凭这个就猜测英国人说的是法语,那就大错特错了。而且,文特里斯所遇到的单词对他来说毫无意义,只是提供一些证据支持 B 类楔形文字是一种迄今为止未知的语言。在工作笔记 20 中,他没有忽视希腊语的假说,但他把它列为"琐碎的枝节"。他下结论说:"如果继续工作下去,我怀疑破译迟早会陷入僵局,或者消失在它的荒诞中。"

尽管他疑虑重重,文特里斯确实继续他用希腊语破译的工作。当工作笔记 20 还在发放时,他开始发现更多的希腊单词。他能识别出 poimen(牧羊人), kerameus(制陶工人), khrusoworgos(金匠)和 khalkeus(铜匠)。他甚至翻译了几句完整的短语。到现在,再没有破译荒诞的威胁挡着他的道路了。三千年来,第一次 B 类楔形文字文字被人诵读,而诵读的语言毫无疑问是希腊语。

在这个进展迅猛的时候,碰巧的是,文特里斯被 BBC 邀请去讨论迈诺斯文字之谜。文特里斯认为这是向大众公布他的发现的理想时机。在一段平淡的关于迈诺斯历史和 B 类楔形文字的讨论后,他做出了具有革命意义的宣告:"在过去的几个星期,我得出结论,克诺索斯和皮劳斯的碑文是希腊文,一种非常难的古希腊语,它比荷马还早五百年。而且写的形式也非常简略。但不论如何,它是希腊文,这一点毫无疑问。"约翰·查德威克是这次谈话的听众之一,他是剑桥大学的教授,而且自从 20 世纪 30 年代,他就对破译 B 类楔形文字非常有兴趣。二战期间,他的工作是亚历山德拉的一名密码

破译员。在那儿,他成功的破译了意大利的密码,此后,他转到布莱里利庄园工作,在那儿,他破译了日本的密码。战后,他又一次试图破译 B 类楔形文字,他运用上他在破译军事密码中所学到的技巧,不幸的是,他取得的成绩很少。当他听到收音机中的访谈时,他完全被文特里斯明显荒谬的宣告惊呆了。查德威克和许多其他听到广播的学者一样,根本不把这个业余者的工作看在眼里。然而,身为希腊语教员,查德威克意识到许多关于文特里斯工作的问题将疾风骤雨般地落到他的头上,为了准备回答这些问题,他决定详细地研究文特里斯的工作。他取得了一份文特里斯工作笔记的副本。他仔细的检查它们,希望它们满是漏洞。然而,几天后,这位怀疑的学者变成了文特里斯 B 类楔形文字是希腊语理论的第一批支持者之一。查德威克非常欣赏这位年轻的建筑师:他的脑筋以一种令人吃惊的速度工作,你的话刚到嘴边,他已经知道你要说的是什么了。他对事情的状况有着敏锐的观察力和理解力,如迈锡尼文明对他来说,并非是抽象的符号,而是他可以理解的活生生的人们。他自己曾致力于解决这个问题的视觉方法,他迫使自己对文字的视觉形象异常熟悉,以至于在他破译这些文字前,大量的视觉形象深深地烙在他的脑袋里。但是,只有画面上的记忆是不够的,他建筑师的训练对他帮助很大。建筑师眼中的建筑物并不仅仅是正面的一些装饰物和结构的特色;他看到的是更底层的,外表之下的东西,他能分辨出建筑模式的显著部分,如结构元素以及建筑物的框架。所以,文特里斯也能分辨出神秘符号的令人迷惑的不同变体,以及这些变体的相同的模式。正是这个品质,从杂乱无章中看出规律的能力,使伟人的工作卓越超群。

然而,文特里斯缺少一项专业技艺,即对古希腊的通彻了解。文特里斯的希腊语的正式教育仅仅是小时候在斯陶学校学的一门课。因此,他没法完全利用他的突破。比如说,他不能解释一些破译的单词,因为它们不在希腊语词汇表中。查德威克的专长是希

腊哲学以及希腊语言演化的研究,他的专长使他能够识别出这些单词问题是以一种非常远古的希腊语形式出现的。文特里斯和查德威克形成了一个完美的合作。

荷马时期的希腊大约是在3000年前,而B类楔形文字的希腊比它还要早500年。为了翻译B类楔形文字,查德威克必须推断出从古希腊语的诞生到B类楔形文字的单词都发生了什么。他不得不考虑以下三个语言发展的方式。首先,随着时间的流逝,单词读音的变化。比如,单词"bath - pourers(喷头)"从B类楔形文字中的lewotrokhowoi到了荷马时期演变成了loutrokhooi。其次,语法也有变化。比如,在B类楔形文字中所有格的结尾是 - oio,但是在经典希腊语中它被替换成了 - ou。最后,词汇可能会有戏剧性的变化。有一些单词出现了,有一些单词消失了,还有一些的意思改变了。在B类楔形文字中harmo的意思是"wheel(轮子)",在后来的希腊语中,它的意思变成了"战车"。查德威克指出这类似于现代英语中用"wheels(轮子的复数)"表示汽车。

有了文特里斯的破译技巧和查德威克古希腊的专业知识,这对二重唱继续说服全世界相信B类楔形文字的的确确是希腊语的文字。翻译的速度日益加快。在查德威克对他们工作的报告《B类楔形文字的破译》中,他写道:"密码术是一门推导和受控实验的科学,从形成到检验,而后时常被抛弃。但那些通过检验的残余物继续生长,直到实验者某一天感到脚踏实地。"他比喻说:把藏匿于伪装下琐碎枝节的意义拼凑在一起,密码便破译了。可能,对这一刻最好的形容是希望的指引看起来走得如此之快,以至于你赶都赶不及。这就像原子物理中的链式反应:一旦跃过阈值,反应就自动进行下去了。

此后不久,他们向世人展示了他们在这种文字上的杰作,他们能够用B类楔形文字互通短信。一种非正式的方法可以检测破译的正确性,就是计算文中神灵名字的个数。过去,那些走错路的

破译,毫无疑问地会产生许多没有意义的词,通常会被解释成一个未知的古代神灵的名字。但是,在查德威克和文特里斯的破译文字中只有四个神灵的名字,而且都是已知的神灵。

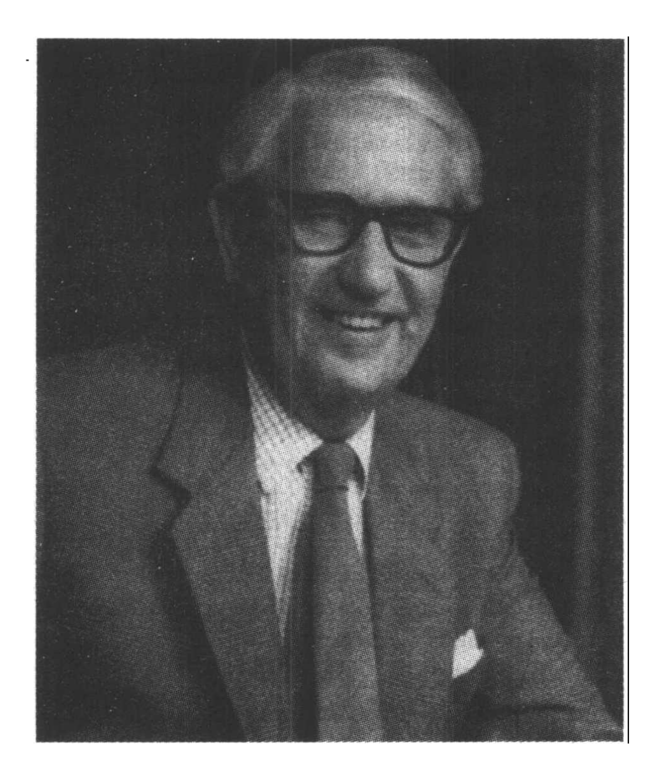


图 61:约翰·查德威克

1953 年,对他们的分析充满信心,他们在一篇论文中总结了他们的工作,简明地取名为《迈锡尼记录中希腊语的证据》,发表在《希腊研究杂志》上。其后,世界各地的考古学家渐渐意识到他们目睹了一场革命。在给文特里斯的一封信中,德国学者恩斯特·斯

迪格概括了当时学界的心情:“我再次强调:您的证明是我所听说的最有趣的密码术,而且是如此的令人着魔。如果您是正确的,那么在过去 50 年中、考古学、人类学、历史和哲学的方法都会被归于荒谬。”

事实证明,亚瑟·埃文斯爵士和他那一代考古学家对 B 类楔形文字的推测大多都是错误的。首先,B 类楔形文字无疑是希腊文字。其次,如果克里特的迈诺斯人写的是希腊文,他们说的很可能就是希腊语,这将迫使考古学家重新认识迈诺斯的历史。现在看来,这个地区的统治者是迈锡尼人,而迈诺斯的克里特只是一个很小的国家,它的国民说着强大的邻国的语言。然而,有证据表明在公元前 1450 年以前,克里特是一个独立的国家而且有着自己的语言。也就是大约在公元前 1450 年,B 类楔形文字取代了 A 类楔形文字。虽然这两种文字看起来很像,A 类楔形文字至今仍未被破译。A 类楔形文字很可能和 B 类楔形文字不一样,是一种消失了的语言的文字。这一切看起来像是大约在公元前 1450 年迈锡尼人征服了克里特,强迫克里特人学习他们的语言,并把 A 类楔形文字改成 B 类楔形文字,使它能够拼出希腊语。

在澄清了历史轮廓的同时,B 类楔形文字的破译也填补了历史的细节。比如,在皮劳斯的考古挖掘中,在这奢侈的宫殿遗址并没有发现贵重的东西。这个宫殿是被火烧掉的,这使一些人怀疑它是被入侵者放火烧掉的,在此之前,入侵者已经把其中的宝物洗劫一空了。虽然皮劳斯的 B 类楔形文字文字没有详细记载这次入侵,但它却提到了为一次防御进攻作准备。一个碑文描述了建立一支特殊军事部队来保卫海岸。而另一个碑文记载了征集铜饰物用来做矛头。还有一个碑文,比前两个更显杂乱,记载了一次特别举行的宗教仪式,其间可能包括把人作为牺牲品。大多数 B 类楔形文字的碑文都是很整洁的,这说明抄写员在写碑文之前都打了个粗略的草稿,草稿用完后就被毁掉了。这个较杂乱的碑文中

间有较大的间隔,半空的行,和溢出到另一边的文字。一个可能的解释是这个碑文是在面临大敌时所刻写的,为的是祈求神灵的帮助。在能够重新刻写它之前,宫殿已成了一片废墟。

有大量的B类楔形文字所记录的文字是清单,记录了日常的交易。它们表明存在一个官僚体制,能与历史上任何一个体制匹敌,并记录了详细的手工制品和农产品的清单。查德威克把这些清单记录比作最后审判日之书。狄尼思·培琪教授是这么详尽形容这些清单的:"绵羊的总数有25000只,但还要记录一只家畜是贡献给了Komawens……我们可以认为播下的每一粒种籽,用掉的每一克青铜,机织的每一根羊毛,下仔的山羊,长肥的猪无不被记录在案。"这些宫殿的记录可能看起来很无聊,但它们生来就有几分浪漫,因为它们与荷马史诗《伊利亚特》和《奥德赛》的联系如此紧密。当克诺索斯和皮劳斯记录它们日常的交易时,特洛亚战争正在进行,而俄狄修斯所用的语言正是B类楔形文字。

1953年6月24日,文特里斯做了一次关于破译B类楔形文字的公共讲演。次日,时代杂志就做了报道。这篇报道的旁边是一篇关于近日征服珠穆朗玛峰的报道。这让人们把文特里斯和查德威克的成就誉为"古希腊考古学的珠穆朗玛峰"。次年,他们决定把他们的工作整理成三册具有权威性的书。其中包括破译方法的描述,300段碑文的分析破译,包含630个迈锡尼单词的词典,几近所有B类楔形文字文字的读音(见表23)。《迈锡尼时期的希腊文卷(Documents in Mycenaean Greek)》完成于1955年的夏天,准备于1956年的秋天出版。然而不幸的是,就在付梓的几个星期之前,1956年9月6日,麦克尔·文特里斯在车祸中意外丧生。当天深夜,在驱车回家的路上,他的车与一辆卡车相撞。地点是在靠近哈特费尔德的路上。约翰·查德威克为他的同事,一位能和钱普里昂媲美的英年早逝的天才,献上悼词:"人们只要在研究希腊历史和希腊语时,人们就会记得他生前所作的工作和他的名字。"

表 23:B 类楔形文字符号和它们相对应的数字和音标

编号	音标	编号	音标	编号	音标
01	*da*	30	*ni*	59	*ta*
02	*ro*	31	*sa*	60	*ra*
03	*pa*	32	*qo*	61	*o*
04	*te*	33	ra_2	62	*pte*
05	*to*	34		63	
06	*na*	35		64	
07	*di*	36	*jo*	65	*ju*
08	*a*	37	*ti*	66	ta_2
09	*se*	38	*e*	67	*ki*
10	*u*	39	*pi*	68	ro_2
11	*po*	40	*wi*	69	*tu*
12	*so*	41	*si*	70	*ko*
13	*me*	42	*wo*	71	*dwe*
14	*do*	43	*ai*	72	*pe*
15	*mo*	44	*ke*	73	*mi*
16	pa_2	45	*de*	74	*ze*
17	*za*	46	*je*	75	*we*
18		47		76	ra_2
19		48	*nwa*	77	*ka*
20	*zo*	49		78	*qe*
21	*qi*	50	*pu*	79	*zu*
22		51	*du*	80	*ma*
23	*mu*	52	*no*	81	*ku*
24	*ne*	53	*ri*	82	
25	a_2	54	*wa*	83	
26	*ru*	55	*nu*	84	
27	*re*	56	pa_3	85	
28	*i*	57	*ja*	86	
29	pu_2	58	*su*	87	

第六章 艾丽丝和鲍勃的公开密钥

第二次世界大战期间，英国的密码破解员比德国的密码制造者棋高一招，主要归功于布莱切里院的员工。他们在院核心部门的领导下，发展出了一套最初的密码破解技巧。除了破解"恩格玛"密码的图灵"炸弹"之外，英国人还发明了另一台密码破解机器——科洛希斯(巨人)。这台机器是为了破解德国的另一种更强大的加密法而制造的。德国人把他们的这种加密法称为德国洛伦茨密码。这两台密码破解机中，决定20世纪后半叶密码术发展的是科洛希斯。

洛伦茨密码用来加密希特勒和他的军官之间的通讯。加密是由洛伦茨S40机完成的。这种机器的操作和"恩格玛"机很相似。但是，洛伦茨密码较为复杂。它给布莱切里的密码破解员提出了更大的挑战。然而，布莱切里的两位密码破解员，约翰·蒂尔特曼和比尔·塔特发现了洛伦茨密码的一个破绽。布莱切里人利用这个破绽，读懂了希特勒的电文。破解洛伦茨密码需要综合各种技术，包括寻找、匹配、数据分析和谨慎的判断。这一切都不是"炸弹"所能做到的。"炸弹"能够高速度运算一个特定的任务，但它们很难变通地应付洛伦茨密码的精妙之处。洛伦茨密码加密的电文不得不通过手工破译，这常常需要经过几个星期的努力，而破译出

来时，电文早已过时了。终于，一位布莱切里的数学家，马克斯·纽曼发明了一种机器破译洛伦茨密码的方法。基于艾伦·图灵的“万能机器”的概念，纽曼发明了一种可以针对不同问题进行自我调节的机器。现在我们称之为可编程计算机。

实现纽曼的设计在技术上看来是不可能的。所以，布莱切里的高级官员搁置了这个计划。幸运的是，一位参加了纽曼设计讨论的工程师汤米·弗劳尔斯无视布莱切里的怀疑，决定开始制造这个机器。在位于伦敦北部多利斯山的邮政部研究中心，弗劳尔斯按照纽曼的蓝图，花了 10 个月的时间造了科洛希斯机器。在 1943 年 12 月 8 日，这台机器被运往布莱切里院。它总共有 1500 个电子管，这比炸弹中用的笨重的电动继电器开关要快得多。更重要的是，科洛希斯之所以快是因为它是可以编程的。事实上，科洛希斯正是现代数字计算机的前身。

科洛希斯连同在布莱切里院的其他东西一起，在战后被毁掉了。参与这项工作的人又被禁止谈论它。当汤米·弗劳尔斯接到命令处理掉科洛希斯的蓝图时，他服从了这项命令，把蓝图烧掉了。世界上第一台计算机的设计图就此消失了。这意味着其他科学家得到了成为计算机发明人的机会。1945 年，宾夕法尼亚大学的 J·蒲利斯普·埃克特和约翰·W·墨西里完成了 ENIAC，它含有 18000 个电子管，每秒能计算 5000 次。几十年来，ENIAC 而非科洛希斯被认为是计算机之母。

密码破译员对现代计算机的诞生做出了重要贡献。在战后，他们继续发展并应用计算机技术以破解各种各样的密码。现在，他们可以利用计算机的速度和灵活性寻找所有可能的密钥直至找到正确的一个。而同时，密码制造者也开始还击，他们利用计算机的威力制造出更加复杂的密码。简言之，战后，计算机对于密码破解者和密码制造者来说都是至关重要的。

用计算机加密一段电文，在很大程度上与传统的加密方法非

常相似。事实上,计算机加密和机器加密(比如,恩格玛机)只有三个重要的区别。首先,密码机受限于实际建造中的困难,而计算机可以模拟出任何无限复杂的机器。比如说,计算机可以用编程来模拟 100 个扰频器的运作,如一些顺时针方向自旋;一些反时针方向自旋;一些每十个字母后消失,其他的在加密过程中越转越快。想建造从事如此复杂运作的机器几乎是不可能的,但在计算机中这种运作却很容易做到,从而使其能发送高保密的电文。

第二个区别简单说来就是速度。电子设备比机器的扰频器运转起来要快得多。一个模拟"恩格玛"机运作的计算机可以瞬时间把一条长电文加密。而同时,计算机也可以在一个合理的时间内用相当复杂的方法加密电文。

第三个区别,也是最重要的区别,计算机加密的是数字而非字母。计算机只处理二进制数。简单说,就是由数字 0 和 1 组成的序列。在加密前,任何电文都要转换成二进制数。这种变换可以通过各种协议完成,比如说 ASCII 码(美国信息交换标准码)。ASCII 码用 7 位的二进制数编码字母表中的字母。到目前,我们只需知道每个 7 位不同的二进制数代表不同的字母,就像莫尔斯码中用点和线代表字母一样。总共有 128(127)种不同的二进制数,所以它们能够编码 128 种不同的字符。这是 ASCII 码能够编码大小写字母(比如 a = 1100001),各种标点符号(比如! = 0100001),以及其他的一些符号(比如 & = 0100110)。

一旦电文被转换成二进制数,计算机就可以开始加密了。

即便我们现在处理的是计算机和数字,而不是机器和字母,加密过程仍然是按照古老的原则来进行的。这些原则包括:替换——电文中的某一成员代表另一成员;换位——电文中成员的位置互换。每次加密,无论多么复杂,都可以还原成一些简单操作的组合。接下来的两个例子说明了计算机加密原理是多么简单。这两个例子分别说明了计算机是怎样实现最简单的替代密码和换位

密码的。

首先，试想我们要加密的电文是 HELLO(你好)，我们用的方法是用计算机实现简单换位密码。在加密前，我们必须根据表 24 中的转换表，把电文翻译成 ASCII 码：

明文 = HELLO = 1001000 1000101 1001100 1001100 1001111

一种简单的换位加密法是把对调第一位和第二位，对调第三位和第四位，依次类推。在这个例子中，最后一位保持不变。因为数字个数是奇数。为了更好地看清楚这次操作，我除去了明文 ASCII 码中间的空格，得到一个序列，并把这个序列与加密后的序列作对比如下：

明文 = 10010001000101100110010011001001111

密文 = 01100010001010011001100011000110111

表 24：ASCII 码与大写字母所换位的二进制数字

A	1000001	N	1001110
B	1000010	O	1001111
C	1000011	P	1010000
D	1000100	Q	1010001
E	1000101	R	1010010
F	1000110	S	1010011
G	1000111	T	1010100
H	1001000	U	1010101
I	1001001	V	1010110
J	1001010	W	1010111
K	1001011	X	1011000
L	1001100	Y	1011001
M	1001101	Z	1011010

这种基于二进制数字换位的有趣性质是，换位不仅仅可以出现在字母本身中，而且，代表字母的比特可以与代表邻位字母的比特发生调换。比如说，交换第七个和第八个数字，分别代表 H 的

最后一个 0 和代表 E 的第一个 1。加密的电文是一个 35 位二进制数字符串,可以发送给接收者,然后通过反换位还原成原来的字符串序列。最后,接收者通过 ASCII 码把序列翻译成原来的电文 HELLO(你好)。

接下来,试想我们希望再次加密同一个电文 HELLO(你好)。只是这一次我们要通过另一种方法——用计算机实现的简单替换法加密。再一次在加密前,我们把电文转换成 ASCII 码。和往常一样,替换是基于发送者和接收者共同达成的密钥。在这个例子中,密钥用 DAVID 的 ASCII 码表示,它是通过下面的方法得以运用的:明文中的每一项与密钥中对应的每一项相"加"。我们可以用两条简单的规则定义二进制数的相加:如果在明文和密钥中的项是一样的,密文中的对应项是 0,如果明文和密钥中的项是不一样的话,密文的对应项是 1:

电文 HELLO(你好)

电文 ASCII 码 10010001000101100110010011001001111

密钥 = DAVID 10001001000001101011010010011000100

密文 00011000000100001101000001010001011

加密电文的结果是 35 位的二进制数,可以发送给接收者。接收者运用同样的密钥,重新做一次反替换,把密文还原成原来的二进制数。最后,接收者用 ASCII 码重新解释二进制数,可以生成电文 HELLO。

计算机加密局限于当时能够使用计算机的群体。这意味着在早期只有政府和军方才能使用。然而,随着科技和工程上的一系列突破,使得更多的人能够使用计算机和计算机加密。1947 年,AT&T 的贝尔实验室发明了晶体管,晶体管成为电子管的廉价替代品。1951 年,有诸如弗兰提这样的公司提供定购计算机的服务,使商务计算机变成了现实。1953 年,IBM 把它的第一台计算机投放市场。4 年后,它推出了 FORTRAN(公式翻译程序语言)

语言,使得普通人也能够编写计算机程序。接着,1959 年,集成电路的发明把计算机带入一个新的时代。1960 年代,计算机的功能更加强大,与此同时,它们的造价也更加的便宜。许多商业公司也能够负担起计算机的费用。这些公司用它来加密重要的通讯,比如说转账和微妙的贸易谈判。然而,随着越来越多的公司采用计算机,公司之间的通讯加密也越来越频繁,密码员遇到了新的问题和困难。这种情况在以前的政府与军队通讯加密中从未遇到过。其中最重要的是标准化的发行。一个企业可以运用特定的密码系统来保障内部通讯安全,但它不能对外面的组织发送秘密电文,除非对方也使用同一套密码系统。最终,1973 年 5 月 15 日,美国国立标准局计划解决这个问题,正式征求一套标准的加密系统方案,能够使企业之间进行秘密通讯。

作为标准的候选对象,许多建立起来的密码算法之一,也是就是称作卢斯福的 IBM 产品。它是由菲思特尔发明的。他是一位于 1934 年来到美国的德国流亡人士。在美国参战时,他尚未成为美国公民,这意味着他一直被软禁在家,直到 1944 年。许多年间,他一直压抑着自己对密码学的兴趣,以免遭到美国当局的嫌疑。他最终在空军的剑桥研究中心开始了密码学研究,不久便发现国家安全局在找他的麻烦。国家安全局负责保持军队和政府的通讯安全,也试图破译外国的通讯。国家安全局雇用了许多数学家,也添置了许多硬件,而且截获了比世界上任何一个组织都多的电文。

国家安全局并不介意菲思特尔的过去,他们只想保持密码研究的垄断。看起来他们的安排取消了菲思特尔的研究计划。1960 年代,菲思特尔到米特尔公司任职,国家安全局继续施压,迫使他再一次放弃工作。菲思特尔终于能在 IBM 的托马斯·J·沃森实验室得以继续他的研究,而没有任何外界的干扰。就是在那儿他发明了卢斯福系统。卢斯福系统的加密步骤如下所述:首先,电文翻译成一长段二进制数字串。然后,以每 64 个数字为一个单位,分

解这段数字串。每个单位数字串分别独立加密。第三步,我们把注意力集中在每个单位数字串上。把 64 个数字像洗牌那样分成两组,每组 32 个数字,分别把它们叫做左 0 和右 0。右 0 中的数字放入“切碎机函数”中,在那儿,数字进行了复杂的替换。然后,把“切碎”后的右 0 加到左 0 上,形成新的一组 32 个数字的排列,称作右 1。把最开始的右 0 标记为左 1。这一系列的操作称为一个“回合”。然后整个操作又重复做一次,不同的只是这一次以右 1 和左 1 开始,得到的数字排列称为右 2 和左 2。加密过程总共要进行 16 个“回合”。这个过程就像是和面一样:试想在一大块面上写着信息,首先,将这块面分成 64 厘米长的小块;然后,挑出其中的一半碾压后折叠起来,再加到另一半上拉长,从而形成一个新的面块。这个过程不断的重复,直到消息文字彻底地被面块混合起来。经过 16 个回合的“揉面”后,密文发送出去。另一端的接收者接到密文后,将加密过程反过来进行,从而解码成明文。

“切碎”的具体实施方法是可以变化的。它取决于发送者和接收者达成的密钥。换言之,只要密钥不同,同样的电文可以用成千上万种不同的方式加密。在计算机密码术中的密钥只是一些简单的数字。因此,加密过程需要发送者将密钥数字和电文都输入卢斯福,卢斯福根据这些输入产生密文。解码则需要接收者把同样的密钥数字和密文输入卢斯福,然后,卢斯福才可以把密文还原成明文。

卢斯福被广泛认为是最好的商务加密产品之一。这样,许多各种各样不同的组织都采用了它。看来,这套加密系统不可避免地将成为美国的标准加密系统。然而,国家安全局又一次干预了菲思特尔的工作。卢斯福是如此的强大,以至于它提供的加密标准方法超越了国家安全局破译密码的能力。国家安全局显然不希望用一种他们不能破译的方法当作美国的标准。对此,有传言说,在允许采用卢斯福成为标准加密系统前,国家安全局要求他们减

少卢斯福的可能的密钥数目,从而,降低了卢斯福的保密强度。

可能的密钥数目是决定加密强度的重要因素之一。对于一个密码破译专家来说,破解密码最简单的方法是揭开所有的密钥,密钥的数目越多,要找到正确密钥的时间就越长。如果仅仅只有1,000,000种密钥,密码破译员只需用一台很快的计算机算上几分钟,就可以找到正确的密钥。不过,如果可能的密钥数目大到一定程度,找到正确密钥的可能性几乎为零。如果卢斯福成为美国标准加密系统,国家安全局希望保证它只能使用一些有限制性的密钥数字。

国家安全局将可能的密钥数目严格限制在10^{18}以内(技术上来讲,这相当于56个比特,因为用二进制解这个数需要56位数字)。看起来,国家安全局相信这样的密钥对民间通讯来讲是安全的。因为没有一个民间组织拥有如此强大的计算机,能够在一个合理的时间内检查每个密钥,但国家安全局拥有世界上最快的计算机资源,刚好能破解卢斯福的密钥。1976年11月23日,56比特版菲思特尔的卢斯福密码机被官方正式采用,称之为数据加密标准(DES)。1/4个世纪后,DES仍然是美国官方认定的加密标准。DES的采用,解决了密码系统标准化的问题。鼓励了许多商家采用密码以保证安全。

DES提供了高效的密码系统,保障商家通讯不受到商务对手的攻击。用民用计算机来破解DES加密的密文几乎是不可能的,因为可能的密钥数目是十分大的。不幸的是,尽管DES很强大,尽管DES提供了加密标准,商家们还要解决另一个密码通讯中存在的问题,这个问题称作“密钥分发”。

试想,银行想通过电话线给客户传送一些保密的数据,但银行很担心电话线被窃听。于是,银行选择了一个密钥,使用DES系统来加密数据。为了解密,客户不仅需要密文,还需要知道密钥。银行怎样才能通知客户密钥是多少呢?显然,不能通过电话线,因

为电话线上可能有窃听者。惟一安全的方法是派人亲手把密钥交给客户,这显然是个费时费力的笨方法。另一种较为可行,但是有一定风险的方法是邮递快件。1970年代,银行尝试着雇用专职的密钥分发员。这些人都经过了严格的选拔,是最值得信任的员工。这些密钥分发员带着一个锁着的箱子走遍了全世界,亲手将密钥交给客户,这些客户将在下一个星期内收到银行传来的加密资料。随着商务网络的逐渐增大,更多的信息需要送出,更多的密钥需要分发,银行发现分发密钥的过程成了可怕的梦魇。分发密钥的日常开支变得无比昂贵。

很久以来,"密钥分发"的问题一直困扰着密码专家。比如,二战时,德国高级指挥部每个月都需要分发《每日密钥》月刊给所有的"恩格玛"机操作员。而且,即使U型潜艇大多数时间都远离基地,它也不得不想办法获得最新的密钥。在早期,文吉尼尔密码的使用者也需要把发送者的密钥交给接收者。无论某种密码从理论上讲是多么的安全,在实际运用中,它都不可避免地遇到了"密钥分发"的问题,这就大大破坏了它的可实施性和安全性。

从某种程度上讲,政府和军队可以通过花费大笔的金钱来解决密钥分发的问题。它们传送的信息是如此的重要,以至于人们为了保证安全性会不择手段。美国政府的密钥是COMSEC(通讯安全局的缩写)掌管和分发的。1970年代,COMSEC每天分发的密钥数以吨计。当装载着COMSEC密钥的船靠港时,密码分发员会到甲板上收集各种卡片、纸带以及软盘和其他一切贮存密钥的介质。然后,把它们分发给客户。

密钥分发看起来是个世俗的问题,但它成了战后密码学家要解决的最重要的问题。如果两个组织需要安全通讯,却需要第三方来传送密钥,这就成了安全通讯最薄弱的环节。对于商家来讲,这个问题就更为突出。如果说,政府能够花大笔的金钱用在密钥分发上以保证它的通讯安全的话,民间组织怎么可能负担起这一

笔昂贵的费用呢?

虽然大家都认为密钥分发的问题是不可能解决的,一群天才还是在 1970 年代中期奇迹般地想出了一个卓越的方案,从而解决了这个“不可能的问题”。他们发明了一种看起来违反一切逻辑的加密系统。计算机改变了密码的实施方式,但是 20 世纪密码学最伟大的革命是发明了密码分发的技巧。实际上,这次突破被认为是两千年来自单码替代密码发明以后最伟大的成就。

上帝青睐愚人

维特福德·笛福是他同时代最热情的密码专家之一。他的外表像一幅鲜明而又有点矛盾的图象。他那一尘不染的外套反映出他在 1990 年代大多数时间受雇于美国巨人级的电脑公司之一,“SUN”公司。目前,他的工作头衔是这家公司的“杰出工程师”。然而,他齐肩的长发和他长长的络腮胡却显示出他的心仍然停留在不羁的 1960 年代。他大多数时间在电脑前,但他的样子看起来似乎即使在孟买的嬉皮村也会同样自在。笛福注意到他的衣着和个性能给他人留下深刻的印象。他是这么说的:“人们总是认为我看起来比我的实际身高要高。这是因为不管一个人多重,他只要活力充沛,就显得高大。”

笛福生于 1944 年,他的早年是在纽约的皇后区度过的。当还是小孩的时候,他就着迷于数学,读的书范围很广,从《橡胶化学公司数学手册》到 G·H·哈代的《纯数学教程》。他在麻省理工大学学习数学,于 1965 年毕业。其后,他先后做了一系列与计算机安全有关的工作。到了 70 年代初期,他逐渐成熟,成为少数几位独立的计算机安全专家之一,一位自由思想者,不受雇于任何大公司或政府。回头看看,他是第一位密码“庞克”。

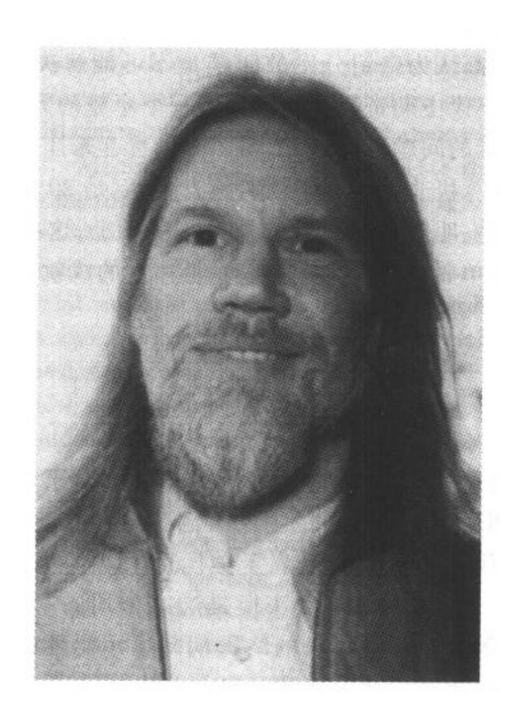


图 62:维特福德·笛福

笛福对密钥分发问题特别感兴趣。他意识到解决这个问题的人将会作为最伟大的密码学家之一而永载史册。笛福对密钥分发问题如此着迷，以至于在他的著作《密码学巨论的问题》中把这个问题单列一章来讨论。笛福的部分动机来源于他对未来有线世界的远见。追溯到 60 年代,美国国防部开始资助一个名叫“先进研究项目机构”(缩写为 APRA)的组织。APRA 中的一个前沿研究项目是寻找一个方案把很远的军方计算机连接起来。这使得一台被毁坏的计算机能够把它的职责通过网络转移到另一台计算机上,其主要目的是使“五角大楼”(美国国防部所在地)计算机设施

在发生核战时更加坚固。而同时,网络使得科学家们也得以互相发送信息,共享远端计算机来做科学计算。APRA 网创建于 1969 年,同年末它连接了 4 个地方。APRA 网的规模逐渐扩大,到了 1982 年它演变成了国际互联网(Internet)。在 80 年代末,非学院和非官方的用户得到允许,可以登录国际互联网。因此,互联网的用户数目激增。今天,1 亿多的用户上互联网交换信息,收发 E - mail。

当 APRA 网还处于它的幼年阶段,笛福就非常有远见地看到信息高速公路和数字革命的到来。将来的某一天,普通人都会拥有他们自己的电脑,而这些电脑将通过电话线连接起来。笛福相信如果人们通过他们的电脑收发 E - mail,那么他们应该得到加密他们信息的权利,以保护他们的隐私权。然而,加密需要安全的交换密钥。如果说政府和大公司对密钥分发感到棘手的话,那么对于大众来说,密钥分发几乎是不可能解决的,而这便剥夺了人们的隐私权。

笛福试想如果两个陌生人在互联网上相遇了,他们怎样才能互发加密的信息呢。他还考虑到了一个人想要通过网络购物的情景。这个人怎样才能发送一封加密的含有信用卡号的 E - mail,而只有接收者才能破解呢?在这两种情况中,似乎双方需要共享密钥,但他们怎样才能秘密地交换密钥呢?这种临时的数字联系和在大众中自发产生的 E - mail 数量是非常巨大的,这就意味着密钥分发是不切实际的。笛福害怕密钥分发的困难会使大众不能拥有使用数字的隐私权,他开始寻找解决这个问题的方法。

在 1974 年,笛福仍是一个自由的密码学家,他应邀到 IBM 的托马斯·J·沃森实验室做一次讲演。他讲述了各种解决密钥分发的战略方案,但他的想法都还处于试验阶段,并且他的听众对解决这个问题的前景也不乐观。对他的讲演惟一积极响应的是阿兰·科黑姆,一位 IBM 的高级密码专家。阿兰提到前不久还有一位密

码学家造访了这个实验室也做了关于密钥分发的讲演。这位讲演者是来自加州的斯坦福大学教授马丁·赫尔曼。当晚,笛福驱车前往5000公里外的西海岸,去会见惟一的一位和他有共同爱好的人。从此,笛福和赫尔曼的合作成为密码学历史上最投机的合作之一。

马丁·赫尔曼于1945年诞生于犹太人居住的布鲁克斯区,但在他四岁的时候,他全家搬到了爱尔兰天主教占多数的小区。这彻底地改变了他的生活态度,据赫尔曼本人说:"其他的小孩上教堂,在那儿他们学到的是犹太人杀害基督徒,所以,他们把我叫做'基督徒杀手',我还被他们殴打。起初,我想和别的孩子一样,能得到圣诞树和圣诞礼物,但后来我意识到这是不可能的,出于自我保护,我的态度变成了'谁想和其他人一样?'。"赫尔曼之所以对密码学感兴趣,也是因为"成为不同的人"的愿望所驱使。他的同事们告诉他,如果他去做密码学研究一定是疯了,因为他面对的将是国家安全局和几十亿美元的资金。他怎么可能发现国家安全局还没有发现的东西呢?即便是他真的发现了一些东西,国家安全局也会把它列作机密的。

当赫尔曼开始他的密码学研究时,他读到了一本名叫《密码破译者》的书,是由历史学家戴维·卡恩写的。这本书首次详细论述了密码的发展。对一个正在成长的密码学家来说,《密码破译者》是一本非常不错的初级读本。《密码破译者》一直是赫尔曼惟一的研究伙伴,直到1974年9月的某一天,他意外地接到了一个来自于名叫维特福德·笛福的人的电话。此时,笛福正在驱车横穿大陆来见他。赫尔曼从未听说过笛福,但是他仍然很勉强答应于当天下午会面半个小时。在这次会面结束的时候,赫尔曼认识到笛福是他所见到的人中知识最为渊博的一位。这种感觉是相互的,赫尔曼回忆道:"我答应了我的妻子要回家看孩子,所以,他跟我一块儿到我家,我们一起吃了晚饭。他直到半夜才离去。我们的性格

并不相同，他比我叛逆性强，但最终个性的不同促使我们能够共事。那次会面对我来说就像一丝新鲜空气。长久在真空中工作是很痛苦的一件事。"

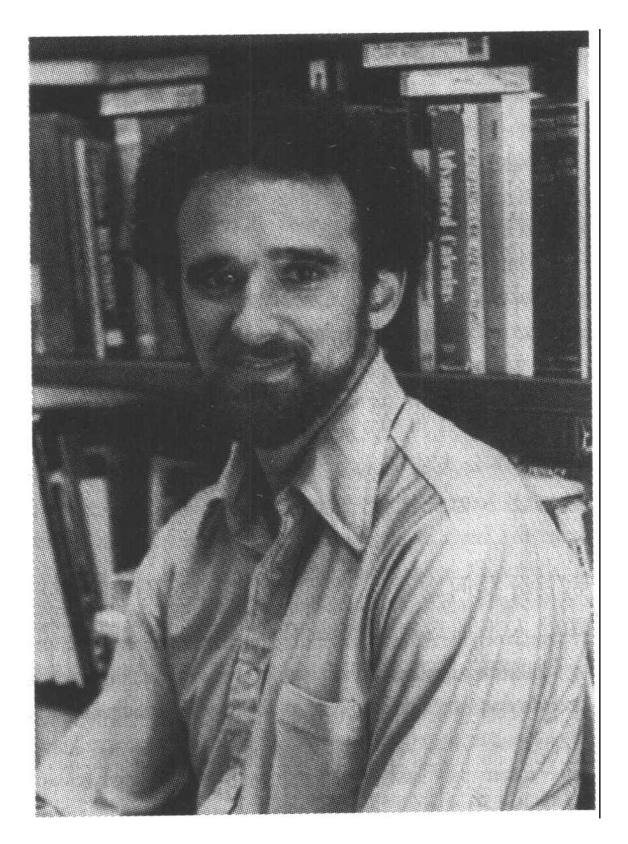


图 63：马丁·赫尔曼

因为赫尔曼没有多少资金，他无法聘请他新的精神伙伴作为研究员。所以，笛福作为一名研究生被录取了。赫尔曼和笛福两

人一起踏上了研究密钥分发问题的漫长征程，不顾一切地试图找到密钥分发问题的简单解决方案，从而替代费时费力的长距离人工传递密钥的方法。在研究过程中，拉尔夫·摩科尔加入了他们的行列。摩科尔是一位非常聪明的流亡者，他原来工作的研究组的教授对他想解决不可能的密钥分发问题毫无怜悯之心。赫尔曼说：

> 拉尔夫和我们一样想当一个愚人。而想做出顶尖的原创研究成就就是成为一个愚人，因为只有愚人才会不断尝试。你有了第一个主意，你无比兴奋，它却失败了。你又有了第二个主意，你又无比兴奋，它再次失败。你有了第 99 个主意，你无比兴奋，它还是失败了。只有愚人才会对第 100 个主意感到兴奋，但往往需要 100 多个主意，才有一个是有用的。除非你愚蠢到能够不断地保持兴奋，否则你会失去目标，你也就没有了足够的动力继续把它做下去。因此上帝青睐愚人。

整个密钥分发问题是一个典型的第 22 条军规，令人左右为难。如果两个人想通过电话秘密交换消息，发送者必须先对信息加密，而为了加密信息发送者必须使用一个密钥，密钥是保密的，接收者为了读取消息必须知道密钥，怎样才能把密钥安全地送到接收者手里呢？简言之，在两个人能够交换秘密（密文）前，他们必须有共享的秘密（密钥）。

当考虑密钥分发问题的时候，为了方便，我们添加了艾丽丝、鲍勃和伊芙三位虚构的人物。这已成为密码学界的标准陈述方法。在一个典型的例子中，艾丽丝想要发送一则信息给鲍勃，或反之亦然。伊芙就试着偷听。如果艾丽丝给鲍勃发私人信息，她在发送信息前必须先加密信息，每次运用一个独立的密钥。艾丽丝

不断遇到密钥分发问题,因为她必须安全地把密钥送给鲍勃,否则,鲍勃无法解码她的信息。解决这个问题的一个方法是艾丽丝和鲍勃每星期会面一次,彼此交换足够的密钥以供以后的7天内使用。用会面来交换密钥显然是安全的,但是极为不便。如果艾丽丝或者鲍勃其中一人病了,整个系统就崩溃了。当然,艾丽丝和鲍勃也可以雇佣密钥分发员,这安全性降低了一点,费用也比较高,但至少减轻了一部分工作。不管哪种方法,看起来密钥分发是不可避免的。2000年来它一直被认为是密码学的定理——一个不争的事实。然而,一个源于思想的实验违反了这一定理。

试想艾丽丝和鲍勃生活在乡村,邮政系统是不安全的,邮政人员会读任何不保险的信件。一天,艾丽丝想发送一条非常私人的信件给鲍勃,她把信件放在一个铁盒中,并把铁盒锁上。她把钥匙保留,并把铁盒通过邮政系统送给鲍勃。但是,当鲍勃收到铁盒时,他没有办法打开铁盒,因为他没有钥匙。艾丽丝可能考虑把钥匙放在另一个铁盒中,锁上这个铁盒并寄给鲍勃。可是没有第二把锁的钥匙,鲍勃仍然不能打开第二个铁盒,因此他也不能取得第一个铁盒的钥匙。惟一解决这个问题的方法看起来只有艾丽丝配一把钥匙并预先把它交给鲍勃,这很可能是在他们共进咖啡的时候。到目前为止,我重新用一种新的形式叙述了一个老问题。在逻辑上避免密钥(钥匙)分发几乎是不可能的。——当然,如果艾丽丝想要把东西锁在一个箱子里,而只有鲍勃能打开,那么她不得不给他配一把钥匙。或者用密码学的方式陈述,如果艾丽丝想给鲍勃发送一则加密的消息,使得只有鲍勃能阅读这则消息,那么她不得不给他密钥。交换密钥是加密不可避免的问题,抑或,并不是这样?

现在,试着勾勒一下以下的情景:和先前的情况一样,艾丽丝想给鲍勃发送一则非常私人的消息。又一次,她把信件装在一个箱子里,加上锁,寄给鲍勃。鲍勃收到箱子后加上自己的锁并把它

寄还给艾丽丝。当艾丽丝收到这箱子时,它加了两把锁。她除去其中她的那把锁,然后,再次寄给鲍勃。这就导致了重要的区别:鲍勃可以打开箱子了,因为箱子上面只有他的那把锁,而他自己有这把锁的钥匙。

这则小故事的意义非同寻常。它说明了两个人可以交换秘密的信息而无须交换密钥。第一次我们看到密钥交换并非密码术中不可或缺的一部分。我们可以用密码术的方式重新诠释这个故事。艾丽丝用她自己的密钥加密一则信息传给了鲍勃,鲍勃对它用自己的密钥再次加密后传回给艾丽丝。当艾丽丝收到双重加密的消息后,她去除了她的那一层加密并传给鲍勃。鲍勃只要除去他的加密就可以阅读信息了。

看来,密钥分发问题是可能克服的。因为双重加密方案不需要交换密钥。然而,建造一个能实施艾丽丝加密、鲍勃加密、艾丽丝解密然后鲍勃解密的密码系统存在着一个非常基本的困难。这个问题是加密和解密的次序。一般来说,加密解密的次序是很关键的,应该满足定理“后进先出”。换言之,最后一个加密的人应该最先解密。在如上的策略中,鲍勃是最后加密的人,那么他应该是最先解密的人,但是艾丽丝在鲍勃之前先解密。我们可以从日常做的小事理解次序的重要性。每天早上,我们总是先穿袜子再穿鞋,而每天晚上,我们总是先脱鞋再脱袜子——在脱鞋之前脱袜子是不可能的。我们也得遵守定理“后进先出”。

一些基本的加密方法,比如说恺撒加密法,是如此简单,以至于次序无关紧要。然而,在 1970 年代,所有复杂加密法的次序都很关键,它们必须满足“后进先出”的规则。如果一则信息先由艾丽丝的密钥加密,然后由鲍勃的密钥再次加密,那么它必须先由鲍勃的密钥解密,然后才可以用艾丽丝的密钥解密。可以说次序对于简单的单字符替换加密法也是至关重要的。我们试想艾丽丝和鲍勃都有自己的密钥,然后我们来看看如果次序颠倒了会发生什

么情况。艾丽丝用她的密钥加密一则信息给鲍勃,鲍勃用他的密钥再次加密密文;然后艾丽丝用她的密钥解密,接着,鲍勃用他的密钥解密。会发生如下的情况:

艾丽丝的密钥

a b c d e f g h i j k l m n o p q r s t u v w x y z
H F S U G T A K V D E O Y J B P N X W C Q R I M Z L

鲍勃的密钥

a b c d e f g h i j k l m n o p q r s t u v w x y z
C P M G A T N O J E F W I Q B U R Y H X S D Z K L V

信息	m e e t	m e	a t	n o o n
用艾丽丝的密钥加密	Y G G C	Y G	H C	J B B J
用鲍勃的密钥加密	L N N M	L N	O M	E P P E
用艾丽丝的密钥解密	Z Q Q X	Z Q	L X	K P P K
用鲍勃的密钥解密	w n n t	w n	y t	x b b x

结果是无意义的。然而,你可以试着把解密的顺序换过来,鲍勃先解密,然后艾丽丝再解密,使它满足"后进先出"的规则,结果会和原文相一致。既然顺序如此重要,那么为什么在前面讲的故事中这种方法如此有效呢?答案是挂锁是不分先后顺序的。我可以在一个箱子上挂上20把锁,然后不分先后顺序解开锁,而最终都可以把箱子打开。不幸的是,加密系统对次序的要求远比挂锁严格。

虽说双重加锁方案没法在真实的密码术中实施,但它激发了笛福和赫尔曼寻找一个可实施的方案来智取密码分发问题。他们花了一个月又一个月的时间,想要找到解决方法。虽然每个方法都以失败而告终,但他们努力不懈。他们把研究的注意力放在各式各样的数学函数上。数学函数是把一个数转化成另一个数的数

学操作。比如说,“加倍”就是一个数学函数,因为它把 3 变成 6,把 9 变成 18。不仅如此,我们可以把所有形式的计算机加密操作看作是函数,因为它们只是把一个数(明文)变成另一个数(密文)。

大多数数学函数被归类成双向函数,因为它们既可做正变化,也可以做逆变化。比如说“加倍”就是一个双向函数,因为既可以很方便的加倍一个数以产生它的倍数,也可以很方便做这个变化的逆变化而使倍数还原成原来的数。比如说,如果我们知道执行加倍函数的结果是 26,我们可以反着执行这个函数得到原初的数字 13。我们可以通过一个简单的日常例子来理解双向函数。我们可以把灯开关看成是一个函数,因为它把一盏普通的灯变成了一盏亮着的灯,这个函数就是一个双向函数。你既可以把一盏灯点亮,也可以把点亮的灯熄掉,从而恢复到最初的状态。

然而,笛福和赫尔曼对双向函数并不感兴趣。他们把注意力集中到单向函数身上,就和它的名字一样,单向函数做正变化很容易,但是逆变化就很困难了。换言之,双向函数是可逆的,单向函数是不可逆的。我们可以再次用日常活动来理解单向函数。把黄颜料和蓝颜料混合起来得到了绿色的颜料,这就是个单向函数。因为把两种颜料混合起来很容易,但却不可能把它们分开。另一个例子是打鸡蛋,因为打破一个鸡蛋很容易,但要再把它还原成原来的状态就困难无比了。因此,单向函数有时也是汉普蒂·邓普蒂函数。

取模算法,有时在学校中也称为时钟算法,是一个单向函数很多的数学领域。数学家把有限的数排成一圈,非常像时钟。比如,在图 64 中展示了模为 7 的“时钟”,其中只含有从 0 到 6 的 7 个数字。作 2+3 的运算时,我们从 2 出发,前进 3 格,得到 5,这和平常的运算一样。但如果我们要做 2+6 的运算时,我们从 2 出发,前进 6 个,绕了一圈,得到 1,这就和平常的运算不一样了。这些运算和结果用以下式中表示:

2 + 3 = 5(模算 7) 和 2 + 6 = 1(模算 7)

取模运算是相对较为简单的。其实我们平常提到时间时都运用到了取模。如果现在是 9 点,我们 8 个小时后开会,我们会说会议开始的时间是 5 点,而不是 17 点。在脑袋中,我们计算了 9 + 8(模算 12)。想像一个钟面,指针指向 9,然后前进 8 格,结束时指针指向 5。

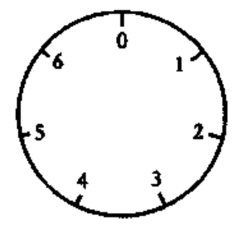


图 64:模算术是在一个有限的数字机上进行的。它可以被想像成一个钟表上的数字。在这种情况下,我们可以算出 6 + 5 模算 7,从 6 开始向前移 5 格,我们可得到 4。

9 + 8 = 5(模算 12)

数学家采取了以下简单的方法来取代钟面。首先,用常规的方法计算算式。然后,如果我们想知道(模算 x)的答案,我们把算式结果除以 x,记下余数。这个余数就是算式(模算 x)的结果。比如,计算 11×9(模算 13),我们采取如下的步骤:

11×9 = 99

99 ÷ 13 = 7 余 8

11×9 = 8(模算 13)

函数在模运算环境中的作用会变得不可捉摸,这使得它们可能变成单向函数。如果我们把一个简单的函数的常规运算和它的取模运算相比较,这一切就变得更加明显了。在前者的环境中,函数是双向的,很容易做逆运算;然而在后者的环境中,函数变成单向的了,而且不能做逆运算。我们把函数 3^x 作为例子来讨论。这个函数的意思是,取一个数 x,然后把 3 自身相乘 x 次,得到一个新的数。比如说,当 x = 2 时,我们运算这个函数:

$3^x = 3^2 = 3 \times 3 = 9$

换言之,这个函数把2变成了9。在常规运算中,随着x的增大,函数的结果也增大了。这使得把结果还原成原初的数较为容易。比如说,如果结果是81,我们可以推出x为4,因为$3^4 = 81$。如果我们弄错了,把x猜成了5,我们计算$3^5 = 243$,这告诉我们的猜测太大了。我们可以减小数字,猜测x为4。我们就可以得到正确的答案了。简言之,即使我们猜错了,我们也可以得到正确的x值,因此,函数是可逆的。

然而,在取模算法中,同样的函数的作用却不这么明显了。试想我们遇到这样一个问题,我们已知3^x(模算7)得1,我们要求x的值。对此我们毫无头绪,因为我们对取模运算并不熟悉。我们可以猜测x值为5,计算3^5(模算7)的结果,答案是5。假设我们要得到1,那么,我们可以减小x值为4,再尝试计算一次,但结果却往相反的方向跑,真正得到的结果却是6。

在常规的运算中,我们测试数字并且能够感知我们是"冷"还是"热"。在取模运算的环境中,我们得不到任何线索,做函数的逆运算变得异常的困难。时常,惟一做取模运算函数的逆运算的方法是做一张表,计算许多x值,直到找到正确的一个x值。表25列举了函数在常规运算和取模运算中不同的结果。它非常明白地表明了函数在取模运算中表现的不可捉摸性。虽说当数字较小时,建表虽显麻烦,但仍然可行,可如果我们要建一个像453^x(模算21997)函数的表时,这几乎是不可能的。这就是一个典型的单向函数,因为我们可以取一个x值并很方便的计算出结果。但如果我给你一个结果,比如5787,你想要知道我取的是哪个x值就困难得许多了。我只需要花几秒钟就可以计算出结果5787,而你却需要用几个小时制作一张表来推出我用的x值。

表 25:函数 3^x 在正常数学(第 2 行)和模数学(第 3 行)里相加。函数在正常数学里持续增加,但在模算术里却极为不确定。

x	1	2	3	4	5	6
3^x	3	9	27	81	243	729
3^x(模算7)	3	2	6	4	5	1

经过两年的取模运算的单向函数研究,赫尔曼愚蠢的执着终于开始有了回报。在 1976 年的春天,他触及到了解决密钥交换问题的方案。经过半个小时的疯狂涂写,他证明了艾丽丝和鲍勃可以达成一个密钥而不需要会面。从而,推翻了维系了几个世纪的定理。赫尔曼的想法基于形如 Y^x(模算 P)的单向函数。开始,艾丽丝和鲍勃达成 Y 和 P 的取值,几乎所有的数值都可以,但也存在一些规定,比如 Y 要比 P 小,这些值是不必保密的。所以艾丽丝可以用电话通知鲍勃,比如说 Y = 7,P = 11。我们稍后可以看到,即使电话线不安全,伊芙听到了这对话也不打紧。艾丽丝和鲍勃现在都同意使用单向函数 7^x(模算 11)。此刻,他们不需要会面就可以开始构建一个密钥了。因为他们的工作是并行的,我用表 26 的两个竖栏来表示他们的步骤。

仔细阅读表 26 的步骤,你会发现,不需要见面,艾丽丝和鲍勃也得到了同样的密钥。他们可以用它来加密信息。比如,我们可以用他们的数字 9 作为 DES 加密系统的密钥。(实际上,DES 的密钥数是很大的,表 26 的过程中真实使用的数也是非常大的,这样,才能得到一个合适的大的密钥数。)运用赫尔曼的策略,艾丽丝和鲍勃就可以达成同一个密钥,而不需要会面彼此耳语了。这非凡成就使得密钥可以通过普通的电话就能达成。但如果伊芙窃听了这个电话,她能知道这个密钥吗?

表 26:普通的单方向函数 Y^x(模算 P).艾丽丝和鲍勃为 Y 和 P 取值,并由此得到相同的单方向函数。7^x(模算 11)。

	艾丽丝	鲍勃
第一步:	艾丽丝选择了一个数字,比如 3,我们用 A 表示这个数字。	鲍勃选择了一个数字,比如 6,我们用 B 表示这个数字。
第二步:	艾丽丝将 3 放入单向函数,并得到 7^A(模算 11)的结果。7^3(模算 11) = 343(模算 11) = 2。	鲍勃将 6 放入单向函数,并得到 7^B(模算 11)的结果。7^6(模算 11) = 117649(模算 11) = 4。
第三步:	艾丽丝将运算所得的结果记为 α,并把她的结果,2,传送给鲍勃。	鲍勃将运算所得的结果记为 β,并把她的结果,4,传送给艾丽丝。
交换:	通常来说,这是最关键的时刻,因为艾丽丝和鲍勃正在交换信息,并且对伊艾来说,这是一个偷听,并得到详细信息的机会。但无论怎样,很显然伊艾的偷听对最终保密系统的安全没有任何影响。艾丽丝和鲍勃可以在电话中达成 Y 和 P 的取值,并且伊艾可以窍听被交换的两个数字,2 和 4。但这些数字却不是密钥,所以伊艾知道了这些数字也没有关系。	
第四步:	艾丽丝得到了鲍勃的结果,并得到了 β^A(模算 11):4^3(模算 11) = 64(模算 11) = 9。	鲍勃也得到了艾丽丝的结果,并得到了 α^B(模算 11):2^6(模算 11) = 64(模算 11) = 9。
密解:	多么不可思议呀!艾丽丝和鲍勃得到了共同的结果,9,这就是密钥!	

让我们从伊芙的角度来看看赫尔曼的方案吧。如果她窃听了电话，她只知道以下的事实：函数是 7^x(模算 11)，艾丽丝发送 $\alpha=2$，鲍勃发送 $\beta=4$。为了找出密钥，她必须和鲍勃做的一样，在已知 B 的情况下把 α 变成密钥，抑或，和艾丽丝一样，在已知 A 的情况下把 β 变成密钥。可是，伊芙并不知道 A 或者 B 的值，因为艾丽丝和鲍勃并没有交换这些数字，而是把它们作为秘密保留起来。伊芙对此毫无办法。从理论上说她惟一的希望是她可以通过 α 推出 A，因为 α 是 A 通过函数运算的结果。而且伊芙是知道这个函数的。或者她可以通过 β 推出 B，因为 β 是 B 通过函数运算的结果，同样，伊芙也知道这个函数。不幸的是，函数是单向的，所以，艾丽丝把 A 变成 α 很容易，鲍勃 B 把变成 β 也很容易，可是，伊芙要想把这个过程反过来，却困难无比，尤其是数非常大的时候更是如此。鲍勃和艾丽丝正好交换了足够的信息来建立一个密钥，而仅仅凭这些信息，伊芙是不可能推出这个密钥的。我们可以用一个形象的比喻来说明赫尔曼的方案，我们想像一种密码是用颜色作为密钥的。首先，我们假想每个人包括艾丽丝、鲍勃和伊芙都有一个三升的罐子，每个罐子中都有一升黄色的颜料。如果艾丽丝和鲍勃想要达成一个密钥，他们每个人把一种秘密颜色的颜料加一升到各自的罐子里。艾丽丝可能加的是一种特殊的紫色，而鲍勃可能加的是深红色。每个人把各自混合好的颜料寄给对方。艾丽丝得到鲍勃的混合颜料后往里面加入一升的自己的秘密颜料。同样，鲍勃得到艾丽丝的混合颜料后也往里面加入一升的自己的秘密颜料。这样，鲍勃和艾丽丝的罐子中得到了同样的颜色，因为其中都有一升黄色的颜料，一升鲍勃的秘密颜料，和一升艾丽丝的秘密颜料。这种混合了三种颜料的颜色正好可以用作密钥。艾丽丝不知道鲍勃加的是什么颜色，鲍勃也不知道艾丽丝加的是什么颜色，但是他们得到了相同的结果。而同时，伊芙就更狂躁不安了。即使她窃取到了运输途中的罐子中的颜色。她也不能推出最

终罐子中的作为密钥的颜色。她可以知道黄色和鲍勃的秘密颜色的混合色，也可以知道黄色和艾丽丝的秘密颜色的混合色。但她不可能通过这些混合色知道鲍勃或者艾丽丝的秘密颜色。因为颜色的混合是单向函数。

赫尔曼的突破发生在他深夜在家工作的时候。所以，当他完成计算时，给笛福和摩科尔打电话已显得太晚了。他只有等到第二天早上再给世上剩下的惟一两个相信密钥分发能够解决的人宣布他的发现。“缪斯女神对我轻声耳语，”赫尔曼说，“但我们是一块儿搭建基础的。”笛福立刻意识到赫尔曼突破的威力，他说：“马特用异常简单的方式解释了他的密钥交换系统。一边听他讲，一边我意识到这个想法困扰在我的脑海里已有一段时间了，但我一直无法突破它。”

虽然笛福 - 赫尔曼 - 摩科尔密钥交换方案能够使艾丽丝和鲍勃通过公开的讨论建立一个秘密，作为科学史上最违反直觉的发现之一，这个发现也迫使密码构造重新编写加密方式。1976 年 6 月的国家计算机会议上，笛福、赫尔曼和摩科尔公开陈述了他们的发现，这可惊呆了许多密码学家。次年，他们申请了专利。自此以后，艾丽丝和鲍勃不需要为了交换密钥而会面了。艾丽丝只需给鲍勃打个电话，和他交换几个数字，就可以建立一个密钥，然后用它加密即可。

虽然笛福 - 赫尔曼 - 摩科尔密钥交换是一个巨大的进步，但这个系统并非完美，因为它很不方便。试想艾丽丝住在夏威夷，她给住在伊斯坦布尔的鲍勃发封 E - mail。鲍勃很可能在睡觉，但对于艾丽丝来说 E - mail 的乐趣是她可以在任何时候发送。它会静静地等在鲍勃的计算机里面，鲍勃醒来时就会见到。然而，如果艾丽丝想加密她的信息，她需要和鲍勃达成一个密钥。这需要和鲍勃同时在网上才成，因为这个过程需要相互交换信息的。为了提高效率，艾丽丝不得不等鲍勃醒来。否则也可以这样，艾丽丝把

她的一半密钥寄给鲍勃,12 个小时后等鲍勃的回答。在此时,密钥就达成了,如果艾丽丝还没睡的话,她就可以用它加密信息,发给鲍勃了。无论哪种方法,赫尔曼的密钥交换方案都延迟了 E-mail 的及时性。赫尔曼攻破了密码学的信条之一,证明了艾丽丝和鲍勃不需要会面也能达成密钥。下面,另一位人物发现了密钥分发问题的更有效的解决之道。

公共密钥密码术的诞生

玛丽·费希尔从未忘记维特福德·笛福第一次邀她出来约会的情景。她回忆道:"他知道我是一个太空迷。所以,他提议我们去看一次火箭发射。维特说他当晚要出发去看一次空间实验室的发射。所以我们整晚驱车,半夜 3 点才抵达目的地。有人把我们拦住,他们说凭维特的信誉他可以进去,但不知道我是谁。所以,维特对他们说我是他的妻子。那是 1973 年 11 月 16 日。"最终他们的确结婚了。早年的时候,玛丽支持她的丈夫做他的密码冥想的时候,笛福仍只是一个研究生,那意味着他的工资是非常可怜的。玛丽,一个受训的考古学家,为了生计只好在英国石油部门工作。

当马丁·赫尔曼发展他的密钥交换方法的时候,笛福致力于用一种完全不同的方法来解决密钥分发问题。他时常长时间地苦思冥想,却毫无结果。1975 年,一次冥想后,他是如此的受挫,他告诉玛丽他是一个失败的科学家,一文不值。他甚至给玛丽说她应该找别的男人。玛丽告诉他,她对他有信心,然而就在两个星期后,笛福想出了绝妙的主意。

他仍然记得这个主意是如何闪过他的脑中的,而且差点儿让它跑掉。他说:"我下楼去买一杯可乐,几乎把这主意忘掉了。我当时记得我在思考很有趣的事情。但记不起是什么了。然后它再

次回到我的脑中，我的肾上腺素立即增高了许多。我意识到这是我密码学研究生涯中第一次有价值的发现。在此以前我的密码学工作在我看来完全是技术枝节。"那是在下午发生的，维特不得不等几个小时，玛丽才会回来。"维特等在门口，"玛丽回忆说，"他说他有事要告诉我，他脸上的表情很奇怪。我进了门，他说：'请坐下来，我想和你说话。我相信我有一个重大的发现——我是第一个知道这问题的答案的人。'这一刻我感觉时间突然停止了，我似乎生活在好莱坞的电影中。"

笛福制造出一种新型的密码。这种密码结合了一种被称为"不对称密钥"的密钥。到目前，本书以前所述的加密方法都是"对称"的。这意思是说，解密过程只是加密过程的反演。比如，"恩格玛"机用一个密钥给电文加密，而接收者也需要用同一个密钥给密文解密。同样的，DES 解密时也用同一个密钥反向执行 16 个回合。这样，加密者和解密者必须都知道同样的密钥，他们用同一个密钥加密和解密——他们的关系是对称的。从另一方面说，在一个如前所述的不对称密钥的加密系统中，加密密钥和解密密钥不是相同的。在不对称密码中，如果艾丽丝知道加密密钥，她可以加密一则信息，但她不能解密。为了解密，艾丽丝必须还拥有解密密钥。这种解密密钥和加密密钥的区别使得不对称密码非常特别。在此刻，我们要强调一下，虽然笛福想出了不对称密码的概念，但他并没有想出一个具体的实行方案。然而，仅仅是不对称密码的概念也是具有革命性的。如果密码学家能够天才般地找出一种不对称密码的实行方案，一种能够实现满足笛福提出的要求的加密法，那么，这对艾丽丝和鲍勃的意义都非常重大。艾丽丝可以作出她自己的一对密钥，一个加密密钥和一个解密密钥。如果我们假设这种加密法是通过计算机实现的，那么加密密钥是一个数字，而解密密钥是另一个不同的数字。艾丽丝可以把解密密钥保密，我们把这个密钥称作艾丽丝的"私人密钥"。然而，她可以把加密密

钥发布,任何人都可以知道,我们把这个密钥称为艾丽丝的"公开密钥"。如果鲍勃想发一则消息给艾丽丝,他可以使用艾丽丝的"公开密钥"加密,然后,艾丽丝收到密文后用她的"私人密钥"解密。同样的,如果其他人想给艾丽丝发信,他们也可以用"公开密钥"加密,而且这些信只有艾丽丝通过使用私人密钥才能解密。

这个系统的巨大的优点是不需要像笛福-赫尔曼-摩科尔密钥交换中那样来来回回地折腾了。鲍勃不需要从艾丽丝那儿获取信息就可以加密一则信息并发送给她了。所有他需要做的只是去找一下艾丽丝的"公开密钥",而且,不对称密码也克服了密钥分发的困难。艾丽丝不需要把"公开密钥"秘密地送给鲍勃。完全相反的是,她希望全世界都知道她的公开密钥。这样,任何人都可以给她发送加密的信息了。而同时,即使全世界都知道了艾丽丝的"公开密钥"。没有一个人,包括伊芙,可以破译给艾丽丝的加密信息,因为公开密钥对于解密是毫无帮助的。事实上,一旦鲍勃把信息加密后,他也没有办法解密。只有拥有"私人密钥"的艾丽丝才能解密这则消息。

这正好是传统的对称密码的反面。在对称密码中,艾丽丝竭尽所能把密钥安全地送给鲍勃。因为解密和加密的密钥是相同的,所以艾丽丝和鲍勃不得不做许多防范工作,以防密钥落到伊芙的手里。这正是密钥分发的结症。

回到挂锁的类比,不对称密码可以这样来理解。任何人只需按一下就可以把锁关上,但只有有钥匙的人才能把锁打开。关锁(加密)是容易的,人人都可以做到,但开锁(解密)只能由有钥匙的人来做了。知道关锁的知识毫无助于开锁。试想,艾丽丝设计了一种锁和钥匙。她拿着钥匙,但她制作了成千上万的锁分发给世界各地的邮局。如果鲍勃想发一个信息给艾丽丝,他把它放在箱子中,去到当地邮局,要一把艾丽丝的锁,用它锁住箱子。现在,他不能打开箱子了,但是艾丽丝收到箱子后,她用她的钥匙就可以打

开这箱子了。挂锁和按一下锁上的过程就相当于用公开密钥加密,因为每个人都可以得到挂锁,每个人都可以用挂锁锁上箱子以发送信息。挂锁的钥匙相当于“私人密钥”,因为只有艾丽丝有钥匙;也只有艾丽丝可以打开锁;也只有艾丽丝可以看到箱子中的信息。

这个系统显得很简单,特别是用挂锁来说明就更显如此。但这距离找到一个数学函数来完成同样的功能以实现这个系统还很远。为了把不对称密码这个概念变成可实行的密码系统,必须有人找到一个合适的数学函数。笛福设想有一类单向函数,在特定的情况下,它们可以被逆运算。在笛福的不对称密码系统中,鲍勃可以通过公开密钥加密信息,但他不能解密——这是单向函数。然而,艾丽丝可以通过私人密钥来解密,得知特殊的信息使她能够很方便的作出逆运算。再次,挂锁是一个很好的类比——关上挂锁是单向函数,因为一般情况下你无法打开它,除非你有钥匙,在这种特殊情况下,过程很容易被逆转。

笛福在 1973 年发表了关于他想法的大纲,希望其他的科学家加入寻找合适的单向函数的行列。单向函数是不对称密码的重要组成部分。开始,大家满怀兴致,到了年底,没有人能找到合适的候选者。随着时间的飞逝,越来越大的可能是这种单向函数根本不存在。看起来笛福的想法只局限于理论,而无法实际运用。无论如何,到 1976 年底,笛福、赫尔曼和摩科尔研究组已经在密码学世界进行了一切彻底的革命。他们说服了其他的密码学家相信密钥分发问题是有可能解决的,而且创造了可行的方案笛福－赫尔曼－摩科尔密钥交换方案。虽然,这个方案有点麻烦,但他们还提出了不对称密码的概念——一个完美的当时还不可行的方案。他们在斯坦福大学继续他们的工作,尝试寻找一种特殊的单向函数使不对称密码成为可能,但他们失败了。然而,远在 5000 公里外的美国西海岸的另一个研究组成功地发现了这种函数,赢得了这

场竞争的胜利。

质数猜想

莱昂拉德·阿德尔曼回忆说："我走进罗·里维斯特的办公室，他手中拿着一篇论文，他开始说：'斯坦福的家伙们……'我说，'这很好，罗，但我还有别的事要说'。我对密码学历史一点都不知道，对他讲的也不感兴趣。"使得罗异常兴奋的论文就是笛福和赫尔曼写的，其中叙述了不对称密码的想法。最终，里维斯特说服了阿德尔曼，使他相信这问题中藏有一些有趣的数学，于是，他们合作寻找能满足不对称密码要求的单向函数。后来，埃迪·沙摩尔也加入了他们之中。他们三个人都是麻省理工大学的计算机科学实验室的研究员。

里维斯特、沙摩尔和阿德尔曼组成了一个完美的小组。里维斯特是一位计算机学家，他吸收新知识、新想法的能力非常强，而且能够把它们运用到似乎不可能的地方。他总保留着最新的科学论文，这使他能够遇上寻找不对称密码单向函数的一些奇怪而极好的候选方案。然而，每个候选方案在某些方面都有一些瑕疵。沙摩尔，另一位计算机学家，能够从蛛丝马迹中看到问题的症结，他在这方面的能力非常出色。他也想出了一些不对称密码的实现方案，但他的想法也不可避免的有些瑕疵。阿德尔曼是一位非常有能力的数学家，他负责挑出里维斯特和沙摩尔的错误，以使他们在错误的道路上少浪费时间。里维斯特和沙摩尔花了一年的时间来尝试各种想法，而阿德尔曼也花了一年时间来把它们一一击落。这个三人组开始失去了希望，但他们没有意识到这个失败的过程是他们研究中重要的一环，慢慢把他们从荒凉的数学领域拉到了一片沃土。终于，他们的努力得到了回报。

1977年4月，里维斯特、沙摩尔和阿德尔曼在一个学生家过逾越节。他们喝了不少的葡萄酒，到了半夜才各自回家。里维斯特无法入睡，躺在沙发上阅读一本数学课本。他开始琢磨困扰他几个星期的问题——有可能创建一个不对称密码系统吗？是否存在这样的单向函数，使得只有接收者能够用他特有的信息把它逆转？突然，脑中的迷雾散去，问题的答案越来越清晰，并逐渐显露出来。后半夜，他一直在把他的想法正规化，到了黎明，他已经卓有成效地写出了一篇完整的科学论文。里维斯特作出了一次突破，但这是和沙摩尔、阿德尔曼一年多合作的结果。如果没有他们，这次突破是不可能的。里维斯特按字母顺序排列论文作者名字：阿德尔曼、里维斯特、沙摩尔。

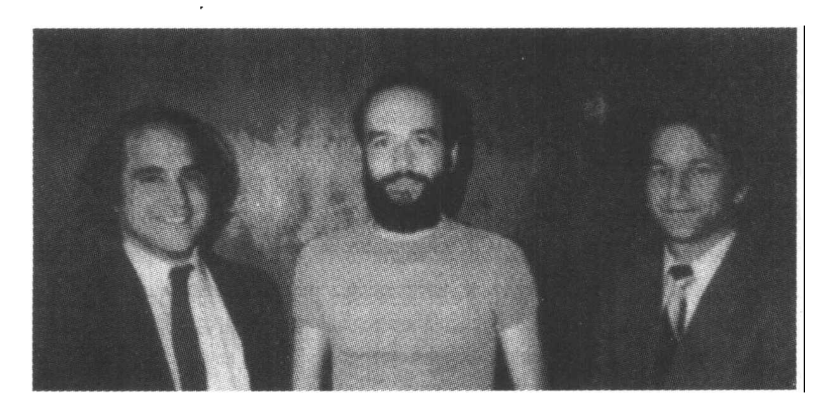


图65：罗·里维斯特，埃迪·沙摩尔和莱昂拉德·阿德尔曼

次日早晨，里维斯特把他的论文交给阿德尔曼，阿德尔曼试图用他常规的方法找出它的瑕疵，但这次他找不出错误。他惟一的意见是对论文作者的名单。“我告诉罗把我的名字从作者名单上拿掉，”阿德尔曼回忆说，“我说这是他的发现，不是我的。但罗拒

绝了,我们不得不对此讨论一下。他们同意让我回家考虑一个晚上,想一下我怎么办。第二天,我给罗提议把我列成第三作者。我当时想这篇论文是我作为作者的最无趣的论文了。"他提醒自己——阿德尔曼不能够再错了。这个系统,称为 RSA(里维斯特、沙摩尔、阿德尔曼)而非 ARS,成为现代密码学中最有影响的密码系统。

在我们探究里维斯特的想法之前,我们先来回忆一下为了建立一套不对称密码,科学家必须做哪些事情:

(1) 艾丽丝必须创建一个公开密钥,鲍勃和其他人可以通过用这公开密钥加密信息传给艾丽丝。因为公开密钥是单向函数,任何人不可能根据它解密给艾丽丝的消息。

(2) 然而,艾丽丝本人应该能解密给她的信息。因此她必须有一个私人密钥——一个特别的信息。通过这个信息,艾丽丝可以很方便地将公开密钥的加密逆转。因此,只有艾丽丝可能解密给她的信件。

里维斯特的不对称密码的核心是一类基于取模的单向函数(前面讲过此类函数)。里维斯特的单向函数可用来加密一则消息——通常是一个数字,而产生密文——是另一个数字。我不打算具体讨论这个函数,但我打算解释它的一个特殊的方面,如果知道数字 N,而这个 N 在特定环境中,就可以把函数逆转,因此,它是作为不对称密码的理想函数。N 是非常重要的,因为它是单向函数中一个可变的数。这意味着不同的人可以选取不同的 N 来创建自己个人的单向函数。为了创建自己的 N,艾丽丝选择两个质数 p 和 q,算出它们的积。质数是只能被它自身和 1 整除的数。比如,7 是质数,因为除了 7 和 1 以外没有数能整除它。同样 13 是质数,因为除了 13 和 1 以外没有数能整除它。然而,8 就不是质数,因为它可以被 2 和 4 整除。

所以,艾丽丝可以选择她的质数为 $p = 17159$ 和 $q = 10247$。

把它们相乘得到 N = 17159 × 10247 = 175828273。艾丽丝选择的N就可以成为她有效的公开密钥了。她可以把N写在她的名片上，抑或发布在互联网上，也可以发表在《公开密钥簿》上。如果鲍勃要发封密文给艾丽丝，他查到艾丽丝的公开密钥，把它加到单向函数的普遍形式中，这函数也是公开的知识。鲍勃现在就有了带有艾丽丝公开密钥的单向函数，可以称它为艾丽丝的单向函数，把信息代入，得到的密文发给艾丽丝。

加密的信息是安全的，因为没有人能够破解它。信息是通过单向函数加密的，根据定义，将加密过程逆转是非常困难的。然而，还有一个问题——艾丽丝怎样能够解密信息呢？为了阅读发给她的消息，艾丽丝必须有一种方法能够逆转单向函数。她必须拥有一些特殊的信息，使她能够逆转函数，解密信息。幸运的是，里维斯特设计了一种单向函数，使如果有人知道制造N的质数p和q，那么他就能把这个函数逆转。虽然，艾丽丝告诉全世界她的密钥是N，但她并没有说p和q的值。所以，只有她知道解密给她的信息，因为只有她能有解密的信息p和q。

我们可以认为N是公开密钥。每个人都可以知道它的值。通过它能够加密信息给艾丽丝。而p和q则是私人密钥，只有艾丽丝知道，通过它能够解密消息。

然而，还有一个问题必须马上说明。如果每个人都知道N，这公开密钥，那么人们当然应该能够通过N推出p和q，这私人密钥，能够读取艾丽丝的信息。毕竟，N是由p和q的积。而事实上，如果N非常大的话，推出p和q是不可能的。这是RSA不对称密码最优美的地方了。

艾丽丝通过选取p和q，相乘它们得到N。这其中最基本的一点是这本身就是一个单向函数。为了说明质数相乘的单向函数的性质。我们可以选取两个质数，比如，9419和1933，把它们相乘。几秒钟我们就可以算出来答案是18206927。然而，如果我们

知道 18206927,要去求它的质因数,这需要我们花去更多的时间。如果你怀疑分解质因数的困难,那么考虑一下下面的情况。我 10 秒钟就可以生成数 1709023。但你用上计算器也要花去一下午的时间才能分解出它的质因数。

这个不对称密码系统,被称为 RSA,是公开密码术的一种。为了检验这种密码的安全性,我们从伊芙的角度来考虑这个密码,尝试着破译艾丽丝给鲍勃的信息。加密一则信息给鲍勃,艾丽丝首先得找到鲍勃的公开密钥。鲍勃选取了两个质数 pB 和 qB 来生成他的公开密钥 NB。pB 和 qB 是他的机密,因为通过它们可以解密密文。但他公开了 NB 等于 408508091。所以艾丽丝把鲍勃的公开密钥加入单向函数中,加密信息后传给鲍勃。收到密文后,鲍勃运用 pB 和 qB 解密密文。而同时,伊芙截获了信息,她惟一的希望是知道 pB 和 qB,通过它们她才有可能破译密文。鲍勃并没有公开 pB 和 qB,但伊芙和别人一样知道 NB 是 408508091,她可以试图从 NB 中推出 pB 和 qB。这个过程是一个分解质因数的过程。分解质因数是非常耗时的,但伊芙究竟要花多少时间来分解 408508091 的质因数呢?有许多种分解质因数的方法,虽然有些方法比另一些方法快一些。但它们都不可避免的需要检查每一个质数,看它是否能整除 NB。比如,3 是一个质数,但它不是 408508091 的质因数,因为它不能整除 408508091。所以,伊芙尝试下一个质数 5,同样,5 也不是 408508091 的质因数。所以,伊芙又得尝试下一个质数。最终,当她算到第 2000 个质数 18313 时,她终于找到了。找到一个质因数后,另一个也相继出来了是 22307。如果伊芙有个计数器,她能每分钟检查 4 个质数,那么这得花去她 500 分钟的时间,相当于 8 个多小时,才能找到 pB 和 qB。换言之,伊芙可以在一天内找到鲍勃的私人密钥。因此,她可以一天内破译给鲍勃的密文。

这个密钥的安全性并不高。但鲍勃可以通过选取更大的质数

的方法提高他私人密钥的安全性。比如说,他能够选取 10^{65}(1 后面跟 65 个 0)数量级的质数。那么 N 的值的数量级就是 $10^{65}\times10^{65}$,也就是 10^{130}了。计算机可以在一秒钟内把两个这么大的质数相乘得出 N。但如果伊芙想从 N 推出 p 和 q 的话,那就要花不是一般长的时间了。究竟多长,那要取决于伊芙的计算机有多快。当时安全专家辛蒙·加芬科尔估计一个拥有 100 兆赫的英特尔奔腾处理器和 8 兆内存的计算机分解 10^{130}数量级的数的质因数要花去 50 年的时间。密码学家考虑了最坏的情况,如果当时全世界的计算机都来破解这个密码,要花多少时间呢?所以,如果 1 亿台个人电脑(1995 年卖出的数量)同时计算,那么,分解 10^{130}数量级的数的质因数需要 15 秒的时间。所以,大家广泛认为要做到真正的保密,必须使用更大的质数。对于银行转账,N 至少大于 10^{308},这比 10^{130}大了 10^{178}倍。一亿台电脑加起来分解它的也要 1000 年的时间。只要 p 和 q 足够大,RSA 是无法被攻破的。

对于 RSA 加密系统惟一的警告是,在未来人们有可能发现更快的分解质因数的方法。想像一下,10 年后,也许就在明天 ,有人发明了快速分解质因数的方法,那么,RSA 就变得无用了。然而,两千年来,数学家一直不断努力想找到分解质因数的捷径,都没有成功。分解质因数仍然是一个耗时的工作。大多数数学家相信分解质因数天生就是一个耗时的工作,而有某一数学定理限制了数学家们不可能找到它的捷径。我们就当他们是正确的。RSA 在可见的未来中,还是一个很安全的加密系统。

RSA 系统的最大优点是它完全摆脱了传统密码中的密钥分发和交换的困扰。艾丽丝不必为传递给鲍勃密钥的安全而担心了。她也不用担心伊芙会在途中截获密钥。事实上,艾丽丝根本不在乎谁能看到公开密钥——越多人看到,她越高兴。因为公开密钥只有助于加密,而非解密。惟一保密的是用来解密的私人密钥,艾丽丝独自保留着这个秘密。RSA 于 1977 年 8 月公布。当

时，马丁·加德纳在《美国科学人》的数学游戏专栏中写了一篇名为《一种新的密码，要几百万年才能破解》的文章。在说明了公开密钥是如何运作之后，加德纳给读者提出了一个挑战。他公布了密文和密文的公开密钥：

N =

114 381 625 757 888 867 669 235 779 976 146 612 010 218 296 721 242 362 562 842 935 706 935 245 733 897 830 597 123 563 958 705 058 989 075 147 599 290 026 879 543 541

挑战是分解 N 成 p 和 q，然后用它们来解密信息。奖金是 100 美元。由于篇幅限制，马丁·加德纳没有具体陈述 RSA 的本质。他叫读者们写信给麻省理工大学的计算机科学实验室索要技术资料。里维斯特、沙摩尔和阿德尔曼非常吃惊，因为他们一共收到了 3000 多封来信索要技术资料。然而，他们并没有立即回信，因为他们担心公布他们的想法会对他们申请专利有威胁。当他们申请到专利后，他们开了一个庆祝会，教授和学生在一块吃比萨饼，享用啤酒。而回信也同时寄出了。

对于马丁·加德纳的挑战，花去了 17 年的时间才有人破译出密文。1994 年 4 月 26 日，一个 600 余志愿者的小组宣布他们找到了 N 的质因数：

q = 3 490 529 510 847 650 949 147 849 619 903 898 133 417 764 638 493 387 843 990 820 577

p = 32 769 132 993 266 709 549 961 988 190 834 461 413 177 642 967 992 942 539 798 288 533

运用这些私人密钥的数字，他们破译出了原文，是一系列的数字，把这些数字转化成字母后，得到的文字是“具有魔力的词是易受惊的鱼鹰”。这个分解质因数的问题分给了 600 个志愿者，他们来自世界各地，包括遥远的澳大利亚、英国、美国和委内瑞拉。他们利用业余时间在他们的个人工作站、大型和超级计算机上计算，

每人负责问题的一部分。世界各地的计算机终于解决了加德纳的挑战。即使是归功于许多计算机的并行运算,一些读者仍然会感到惊奇,为什么能在这么短的时间内破解 RSA 系统呢? 这里需说明,马丁·加德纳所用的 N 相对较小。数量级只达到了 10^{129}。而今,RSA 的用户选择更大的质数产生更大的 N。以至于全世界的计算机一起来运算也要花上比宇宙年龄还要长的时间才能破密。

公开密钥密码学的另一个历史

近 20 年来,笛福、赫尔曼和摩科尔因为发明了公开密码的概念而名扬天下。而同时,里维斯特、沙摩尔和阿德尔曼因发明了 RSA,完美地实现了公开密码而功成名就。然而,最近的一个声明意味着历史可能会被改写。据英国政府声称,他们在切尔特汉姆的政府通讯总部很早就发明了公开密钥密码术。这个最高机密的密码术是由战后的布莱切里庄园的余部发明的。这个故事里充满着许多天才的智慧和无名的英雄壮举,而政府却把它掩盖了几十年。

这个故事开始于 60 年代。那时,英国军方开始担心密钥分发问题。展望 70 年代,当时的英国高级军官试想了这样一幅图景,由于收发机的小型化以及成本的降低,意味着每个士兵都可以通过无线电与长官取得联系。通讯广泛化的好处是非常巨大的,但如果通讯需要加密,那么密钥分发问题就变得不可忍受了。这时候正处在对称密码学的时代,所以同一把密钥必须安全地递给密码系统网络中的每一个成员。通讯的扩展最终会因为密钥分发的困难而止步不前。1969 年年初,英国军方请求詹姆斯·埃利斯,一位前英国政府的密码专家,找到一种能应付密钥分发问题的方法。



图 66:詹姆斯·埃利斯

埃利斯的个性有点古怪。他很骄傲地吹嘘他在出生前就绕着地球转了半圈——他是在英国受孕的,却是在澳大利亚出生的。然后,还是个婴儿时,就返回到伦敦,在西区长大,一直到 20 年代末。在学校里,他的主要兴趣是科学。他在皇家学院深造物理学,其后,他加入了多利斯山的邮政研究中心。正是在这儿,汤米·弗劳尔斯制造了科洛希斯,它是第一台密码破解机器。多利斯山的密码学分部最终被政府通讯总部所接收。所以,1965 年 4 月 1 日,埃利斯到了切尔特汉姆加入了新组建的通讯电子安全组。这个组是政府通讯总部的一个特殊部门,它负责保证英国通讯的安

全。因为这牵涉到英国国家安全,所以,埃利斯宣誓在他的事业上保持缄默。虽然,他的妻子和家人知道他在政府通讯总部工作,他们却一点也不知道他的发明,更不知道他是这个国家中最为出色的密码破解专家之一。

虽然他的密码破解技巧非常出色,但埃利斯从未掌管过任何政府通讯总部的重要部门。他非常卓越,但他也同样不可预料,个性内向,不是一个能够自然跟团队合作的人。他的同事理查德·沃尔顿这样回忆到:"他是一个怪僻的同事,他并不太适合做政府通讯总部的日常工作。但如果说到新想法,他是出类拔萃的。你有时不得不做一些分类垃圾般的工作,但他是如此的有创见而且总是乐于挑战最难的问题。如果政府通讯总部都是他这样的人,那可是一个不小的麻烦,但比之其他大多数组织而言,我们可以容纳更高比例的像他这样的人。我们的确安置了不少他这样的人。"

埃利斯的一个优秀品质是他拥有广博的知识。他阅读所有手边的科学期刊,而且从不扔掉任何东西。出于安全的原因,政府通讯总部的员工每晚必须收拾他们的桌子,把所有的东西锁在一个抽屉里。这意味着埃利斯的抽屉里装满了各种不为人知的出版物。因此,他得到了一个绰号,名叫"密码古鲁"。如果其他研究员遇到无法克服的问题,他们会来敲他的门,寄希望于他的博学和原创能力能帮他们提供一个解决方案。可能就是因为这样的声誉,他才成为解决密钥分发问题的候选人。

密钥分发费用早已涨得很高了,而且成为扩大加密的限制因素。即使减少 10% 的密钥分发费用,都将大幅减少军队的安全预算。然而,埃利斯并非逐步一点点解决这个问题,而是立即开始寻找一种彻底完全的解决方案。他总是用提问的方法去寻找问题的解决方法:"这真是我们想要的吗?"沃尔顿说:"詹姆斯就是詹姆斯。他所做的第一件事就是对共享秘密数据(就是密钥)的需要提出挑战。没有定理说明你必须共享一个密钥。这是个可以提出挑

战的问题。”

埃利斯开始浏览他宝贵科学期刊，对这个问题发起进攻。他发现密钥分发并非密码术中不可或缺的。多年后，他记录了这个瞬间：“那天，我发现了一篇战时的贝尔电话的报告，虽然是一个不出名的作者写的，但其中描述了一个天才关于安全电话通讯的想法，这件事改变了整个事件。文中提议接收者可以通过在线路上加杂噪音来掩盖发送者的讲话，而且接收者最终是可以去除噪音的，因为，只有他知道加的是什么噪音。这个系统实际操作中的明显缺点使它没有得到实行。可是它蕴含着许多有趣的性质。它和传统加密法的区别是，接收者也参加了部分加密的过程……一个想法就这么诞生了。”

噪声是任何影响通讯信号的专业术语。一般来说，它是完全由自然现象造成的。它最明显的一个特征是，它是彻底地随机的，这意味着想从一则消息中去除噪声是非常困难的。如果无线电通讯系统设计得很好，那么噪声的程度就较低，信息就可以听得很清楚，但如果噪声程度高，淹没了信息，就没有任何办法可以恢复信息了。埃利斯提议如果接收者，比如艾丽丝，故意在鲍勃和她的通讯信道上加上噪音，鲍勃就可以给艾丽丝发送信了。即使伊芙窃听了这个通讯，她也没法读懂它，因为信淹没在噪声中了。艾丽丝是惟一一个能去除噪音，读懂信息的人，因为只有她知道所加的噪音是什么。埃利斯意识到，这样的话，不用通过交换密钥就可以实现安全通讯。密钥就是噪音，而且只需要艾丽丝一个人知道就可以了。

在备忘录上，埃利斯详细记录了他的想法：“下个问题是非常明显的。这个想法能实现在普通的加密中吗？我们是否能够产生一个安全的加密信息，使授权的接收者可以阅读，而又不需要密钥交换？在一个晚上这个问题浮现在我的脑中，可能性的理论证明，只花了我几分钟的时间。我们有一条存在定理：不可想像的却是

可能实现的。"(存在定理显示的是某一个概念是可能的,但不去追究它的具体实施方法。)换言之,直到此刻,寻找密钥分发的解决方案仍是大海捞针,而且有可能根本没有针。但是,根据存在定理,埃利斯相信在大海的某个地方针是存在的。

埃利斯的想法与笛福、赫尔曼和摩科尔的想法很相似,只是比他们提前了好几年。然而,没有人知道埃利斯的工作,因为他是英国政府的雇员,而且要发誓保密。到 1969 年末,埃利斯看来已经陷入了僵局,这和斯坦福小组 1975 年陷入的僵局是同样的。他已证明公开密钥是可能的,他也发明了公开密钥和私人密钥的概念。他也知道他需要发现一种特殊的单向函数,这个单向函数在知道某些特殊信息后可以逆转。不幸的是,埃利斯不是一个数学家。他对某些单向函数很熟悉,但他很快意识到单凭己力,是很难再取得更多的进展了。此刻,埃利斯对他的上司陈述了他的理论。他们的反应仍被列为机密文件。但在一次和理查德·沃尔德的会见中,他对我解释了许多交换了的备忘录。他曾经浏览过这些资料:

> 我不能让你看这些文档,因为它们上面仍标有像"最高机密"这样的文字。其中主要讲的是,詹姆斯的想法给高级人员看过了,专家也可以看到。他们认为詹姆斯的想法是完全正确的。换句话说,他们不认为这是胡思乱想。而同时,他们没有办法找到一个实施方案。一方面,他们对詹姆斯的天才想法印象深刻,一方面,他们不确定怎样才能利用它。

接下来的三年中,政府通讯总部的最聪明的头脑努力寻找一个能满足埃利斯要求的单向函数,但毫无结果。接着,1973 年 9 月,一个年轻的数学家加入了这个小组。克利福德·科克斯,刚刚毕业于剑桥大学,是一个纯粹的数学家。当他加入政府通讯总部

时,他对加密和政府军事通讯了解甚少,所以他被分配给了一位导师——尼克·佩特森。克利福德的工作由他指导了几个星期。

六个星期后,佩特森告诉科克斯"一个疯狂的想法"。他讲了埃利斯公开密钥的理论的大概,而且解释道至今没有人能找到合适的数学函数。之所以佩特森告诉科克斯这个想法,是因为这是密码学中最让人兴奋的想法,而不是指望他能够解决这个问题。然而,据科克斯说,那天晚些时候,他就开始工作了:"没有什么特别的发生。我只是想我可以想想这个问题,因为我做过一些数论的研究,自然就想到了单向函数,一些非常难于逆转的函数,而质因数分解很自然地成了我的选择,这就是我的出发点。"科克斯开始阐明一种不对称加密法,这种加密法就是后来为人所知的 RSA 不对称加密法。里维斯特、沙摩尔和阿德尔曼于 1977 年发现了他们的公开密钥密码术的公式,而早在这四年前,这位年轻的剑桥毕业生做出了同样的发现。科克斯回忆到:"从开始到结束,我总共没花半个小时的时间,我对自己很满意,我想'哦,这很好,别人给我提了一个问题,而我解决了。'"

科克斯并不能完全体会他的发现的重要性。他没有注意到这样的事实,政府通讯总部的精英们为这个问题曾付出了三年的努力,更没有意识到他作出了密码术这个世纪最重大的突破。科克斯的天真也可能是他能成功的一个原因,这使他有足够的信心去解决这个问题,而不是一开始就被它唬住。科克斯把他的发现告诉了他的导师。是由佩特森去给上司汇报这个发现的。当时,科克斯还是缺乏自信,仍是一个菜鸟。而佩特森完全能够理解这个问题的内容,而且更善于回答专业问题。很快,许多完全陌生的人开始拜访科克斯,祝贺这个奇迹男孩。其中一个陌生人是詹姆斯·埃利斯,他急于见到把他的梦想实现的人。因为科克斯仍然不能理解这个发现的伟大,这次会面并没有给他留下太多的印象,如今,事隔 20 年后,他对埃利斯已毫无印象了。

当科克斯终于明白他到底做了什么后，他说他的发现会使 G·H·哈代失望的。哈代是世纪初的一位伟大的数学家。在他 1940 年出版的书《一个数学家的辨白》中，哈代骄傲地宣称："真正的数学对战争毫无用处。没有人发现数论对战争有何用处。"真正的数学是指纯数学，比如说数论，这恰恰是科克斯工作的核心。科克斯证明哈代是错的。数论的复杂使将军们能够安全地讨论他们的军事计划。由于科克斯的工作对于军事通讯有着重要的意义，他被告知不准向政府通讯总部以外的人提及他的工作。在最高机密部门工作，意味着他不能告诉他的父母和剑桥原来的同事。他只告诉了他的妻子吉尔，因为她也在政府通讯总部工作。

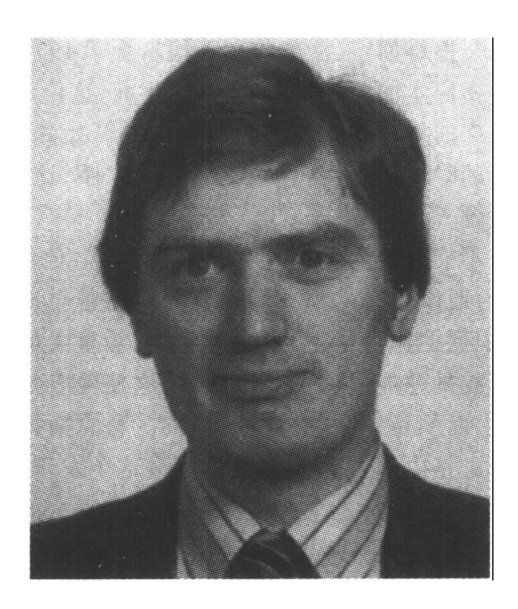


图 67：克利福德·科克斯

虽然科克斯的工作被列为政府通讯部门的机密之一,但它却因为诞生的过早而得不到实现。科克斯的确发现了实现公开密钥密码术的数学函数,但实现这个系统仍存在其他困难。公共密钥加密要求计算机比对称密码术使用的计算机要有更高的性能。在70年代早期,计算机仍然较为原始,不能胜任在一个合理的时间用公开密钥密码术来加密信息。因此,政府通讯总部没法利用公开密钥密码术。科克斯和埃利斯证明了“明显不可能的事”是可能发生的。但没有人能够找到实施它的方法。

又一年,也就是1974年年初,科克斯把他的工作介绍给了马尔科姆·威廉姆生。他是一位刚刚加入政府通讯总部的密码学家。他们俩恰好是老朋友,上的都是曼彻斯特中学,这个学校的校训是“勇于作智者”。1968年两人在校期间,都代表英国参加了在苏联举行的数学奥林匹克竞赛。两人一起从剑桥毕业后分开了几年,但现在他们又在政府通讯总部相聚了。他们从11岁开始就相互交流数学的想法了。但科克斯的公开密钥的想法是威廉姆生听到的最令他震惊的想法。他回忆说:“克利福给我讲述了他的想法,我不能相信,我非常的怀疑,因为如果这能实现的话,那是一件非常特别的事。”

威廉姆生走后,开始试着证明科克斯是错的,公开密钥密码术根本不存在。他检验了这个数学方法,寻找其中藏匿的错误。公开密钥密码术看起来绝妙极了,以至于它都可能不像是真的。威廉姆生决定要找出一个错误,他把问题带回了家。政府工作总部的雇员是不准把工作带回家的,因为他们的工作都是保密的,而家中的环境很可能使工作泄漏出去。然而,问题在威廉姆生的脑中萦绕着,他无法停止想它。他带工作回家,违反了规定。他花了5个小时来寻找错误。“可以说,我失败了。”威廉姆生说,“相反,我找到了另一种解决密钥分发问题的方法。”威廉姆生发现了笛福-赫尔曼-摩科尔加密法。几乎在同一时间,马丁·赫尔曼也发现了

这个方法。威廉姆生的最初的反应表现了他玩世不恭的性格:"这看起来不错,我想,我是否能找出这个方法的错误呢。我想那天我的心情肯定很糟糕。"



图 68:马尔科姆·威廉姆生

1975 年,詹姆斯·埃利斯、克利福德·科克斯和马尔科姆·威廉姆生已经发现了公开密钥密码术所有的重要方面。但他们只能保持沉默。这三个英国人只好暂且休息一下,看到他们的发现在其后的三年陆续被笛福、赫尔曼、摩科尔、里维斯特、沙摩尔和阿德尔曼重新发现。有趣的是,政府通讯总部是先发现 RSA,然后才发现笛福 - 赫尔曼 - 摩科尔密码交换的。而在外面的世界,这个顺序恰恰相反。科学界报道了斯坦福和麻省理工学院的突破。而允许在科学期刊上发表他们文章的研究者们在密码学界成为名人。

如果我们用搜索引擎在互联网上搜索维特福德·笛福，会有 1382 条信息，而克利福德·科克斯却只有 15 条。科克斯对此事的态度令人钦佩，他说："你不必为了取得大众的认同而卷入此事。"威廉姆生对此事也不太关心："我的反应是，'好吧，事情就是这么样。'我得忙我这辈子剩下的时间的事儿。"



图 69：马尔科姆·威廉姆生（左边第二个）和克利福德·科克斯（最右边）参加 1968 年的数学奥林匹克竞赛。

威廉姆生惟一的疑虑是政府通讯总部没有取得公开密钥密码术的专利。当科克斯和威廉姆生发现他们的突破时，政府通讯总部的管理层决定不申请专利，原因有二：一是申请专利意味着得公开他们工作的细节，这与政府通讯总部的宗旨不同。二是，在 1970 年代早期，申请一个数学算法的专利还没听说过。在 1976 年，笛福和赫尔曼准备总结他们的工作申请专利，很明显，他们能够申请成功。在此时，威廉姆生则想公布他们的发现，从而，阻止笛福和赫尔曼得到专利。但是，他的上级不准他这么做，他的上级显然没有看到数字革命的到来和公开密钥密码术的潜力。到了

1980年代初,威廉姆生的老板们开始后悔他们的决定。随着计算机的发展和互联网雏形的形成,使得RSA和笛福–赫尔曼–摩科尔密码交换成了成功的商用密码系统。1996年,RSA数据安全公司,一家负责RSA产品的公司,以2亿美元的高价卖出。

虽然政府通讯总部的工作仍被视为是机密,但已有个其他组织知道了英国取得的突破。1980年代初,美国安全局已经听说了埃利斯、科克斯和威廉姆生的工作。也很可能是通过国家安全局,维特福德·笛福听到了关于英国发现的传言。1982年9月,笛福决定亲自去英国以核实这个传言。他和他妻子来到了切尔滕纳姆,为的是和詹姆斯·埃利斯会面。他们在一个当地的酒馆相遇了,很快,玛丽就被埃利斯出色的人品所打动:

我们坐着聊天,我突然意识到他是你所能想像的最出色的人。我并非是讲他广博的数学学识,而是说他是一个真正的绅士,无比的谦虚,拥有伟大的慷慨精神和教养。我说的教养,意思不是旧式陈腐的那种,而是骑士精神。他的确是个好人,一个真正的好人。他是个高尚的人。笛福和埃利斯谈论了许多不同的话题,从考古学到桶中的老鼠怎么提高苹果酒的味道。但每当谈话转向密码术时,埃利斯就转开话题。最后,当笛福正准备开车离开,他实在不能再忍了,他向埃利斯询问了一个早就想问的问题:"告诉我,你是怎么发明公开密钥密码术的?"接着一个长长的停顿。埃利斯终于轻声说:"好,我不知道我该说多少。让我这么说吧,你们所做的要比我们做的多得多。"

虽然,是政府通讯总部首先发明了公开密钥密码术,但这并不能贬低那些重新发现这个密码术的学者们的成就。正是这些学者们首先意识到了公开密钥密码术的潜力,并且也是他们第一次实施了它。甚至,很可能政府通讯总部永远不会公开他们的工作,因此,阻挡了这种密码术的出现,使数字革命无法达到极致。最后一点,学院学者们的发现是完全独立于政府通讯总部的发现的。在

智力水平上，两次发现是等价的。而且，学院里的研究环境是完全与政府的机密研究隔离的。这些学者们也无法看到藏匿于机密世界后面的研究。而另一方面，政府的研究员总能看到学院的研究工作。我们可以认为这是个信息流单向函数，信息只能自由地往一个方向流动，但不能往另一个方向回流。

当笛福告诉赫尔曼关于埃利斯、科克斯、威廉姆生以及他们的工作时，赫尔曼认为在学院的研究应该作为机密研究史上的一个脚注，同样的，在学院研究史上也要在脚注中说明政府通讯部门研究的成果。然而，当时除了政府通讯总部、国家安全局、笛福和赫尔曼以外，没人知道这项机密的工作。所以，也没有谁想做什么脚注了。

到了80年代中期，政府通讯总部的气氛有所改变，管理层考虑公开埃利斯、科克斯和威廉姆生的工作。公开密钥密码术的数学在大众中早已建立，看来没有什么必要继续保密了。实际上，公开他们公开密钥密码术的研究，只会对英国有利。就像理查德·沃尔德回忆的那样：

> 1984年，我们考虑是否公开我们的工作。我们开始意识到公开一点对政府通讯总部是有好处的。当时正值政府安全市场向外扩张，这远远超出了传统的军事和外交消费者的范围。我们必须取得一些原来与我们没打过交道的组织的信任。我们处于撒切尔主义中期，遇到了一种"政府是坏的，私人是好的"这种社会思潮。所以，我们有意去发表一些论文，但这一切却因为一本彼得·赖特的书《抓间谍者》而搁置下来。

彼得·赖特是一位退休的英国情报官员，其作品《抓间谍者》是他的备忘录。这使得英国政府非常难堪，只好又花了13年的时

间,政府通讯总部才公布他们的工作。也就是埃利斯做出他的工作28年后。1997年克里福德·科克斯完成了他对RSA系统的重要的工作,这个工作是不保密的。它对于更广的人群有着更大的用处,而且,公开它也没有什么安全上的隐患。结果,他被邀请到数学院的会议上去做一次报告。当时在场的有许多密码专家,他们其中许多人都知道科克斯实际上是RSA的发明人,虽然他来做的报告只是谈RSA的一个方面。这就存在有人会问尴尬问题的可能性,如果有人问及“你是否发明了RSA?”,科克斯将如何回答呢?根据政府通讯总部的规定,他不得不撒谎,他只能否认他发明了RSA,这种情形是很荒唐的。所以,政府通讯总部决定改变他们的规定。他们允许科克斯谈论他对公开密钥密码术所作的贡献。1997年12月18日,科克斯发表了他的讲话。将近30年后,埃利斯、科克斯和威廉姆生得到了应有的回报。可惜的是,詹姆斯·埃利斯于一个月前,也就是1997年11月25日逝世,时年73岁。埃利斯加入了生前从未公开其工作的英国杰出密码学家的行列。查尔斯·巴比奇的文吉尼尔密码的破解工作,在他生前就从未公开,因为他的工作对英国军队太有利了,而这个荣誉被记在弗里德里希·凯西斯克的名下。类似的是,阿兰·图灵对战事的贡献与待遇也是不相称的,关于他怎么破解“恩格玛”密码的工作可能永不会发表。

1987年,埃利斯写了一份保密文件,记录了他对公开密钥密码术的贡献。其中有他密码工作看法:密码术是一门特殊的科学。大多数职业科学家旨在发表他们的论文,因为这是实现他们工作价值的途径;相反,密码学的价值是把工作尽量少的暴露给潜在的对手。因此,职业密码学家的工作常常局限在一个封闭的圈子中,在这个圈子中有足够的学术交流,但同时他们的工作是对外保密的。直到历史走到可以证明再保密没有意义后,这些工作才得已公开。

第七章 相当好的隐私

就像维特福德·笛福在70年代预测的那样,我们现在进入了信息时代——一个后工业时代,信息成为了重要的商品。数字信息的交换成了我们日常生活的重要组成部分。实际上,现在每天都有上千万的E-mail(电子邮件)发出,电子邮件很快就会变得比传统的邮件更受欢迎。虽然互联网仍处在它的初级阶段,却已经为数字市场提供了基础设施,电子商务正在兴起。钱在网络空间中流动,据估计,每天有一半的世界生产总值在世界国际银行的金融电信网络(SWIFT)流动。未来,人们可以通过在网上投票选举,政府通过网络管理国家,比如说网上公布税务清单。

然而,信息时代的成功依赖于保护信息的能力,这一切就需要密码术了。密码术为信息时代提供了钥匙和锁。两千年来,加密一直是政府和军队的专利,但如今,它在商务中也扮演着同样重要的角色,未来普通人也需要它来保护自己的隐私。幸运的是,在信息时代来到时,我们已经发展出了异常强大的密码术。公开密钥密码术的发明,尤其是RSA密码的发明,使得密码制造者相对于密码破解者有着明显的优势。如果N的值够大的话,伊芙想要找到p和q就得花上宇宙年龄的时间,因此,RSA加密系统是几乎不可破解的。而且最重要的是,公开密钥密码术不会因为密钥分

发问题而困扰。简而言之,RSA 为我们珍贵的信息提供了几乎不可破解的锁。

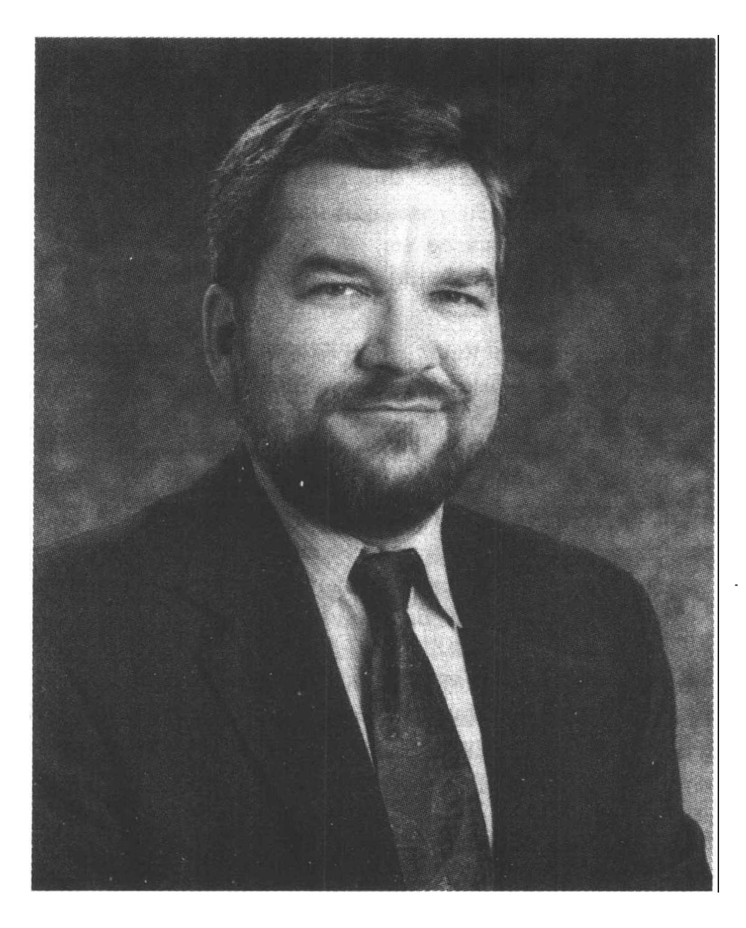


图 70:菲尔·齐默尔曼

但是,同每一种技术一样,加密术也有黑暗的一面。在保护了

守法公民的安全通讯的同时，它也保护了不法分子和恐怖分子的通讯。目前，警方通过窃听通讯的方法来搜集重大案件证据，比如集团犯罪和恐怖活动，但如果罪犯们也用上了不可破解的密码，那么，这一切就不可能了。随着我们进入了21世纪，密码术陷入这样一个窘境，一方面，它要提供给大众，使大众能够享用信息时代的好处；而另一方面，它又不能让罪犯滥用，从而，危害其他的人。现在，关于密码术如何使用的讨论非常激烈，这个讨论是因为菲尔·齐默尔曼的故事引起的。他极力提倡强大密码术的广泛使用，使得美国安全专家惊恐万分，威胁到了腰缠万贯的国家安全局。这使得他成为了联邦调查局的讯问对象和大陪审团的调查对象。

菲尔·齐默尔曼于1970年代中期在佛罗里达的亚特兰大大学就读，学的是物理和计算机。毕业后，他把事业放在了正在兴起的计算机行业中，但1980年代初的一次政治事件改变了他的一生。他不再对芯片技术感兴趣了，而更担心核战的爆发。苏联人侵阿富汗、里根的选举以及愈来愈紧张的冷战局势，给他发出了警报。他甚至考虑举家搬迁到新西兰，他认为那是核战爆发后，世上惟一剩下的几个地方之一。然而，就在他取得护照和签证后，他和他的妻子却去参加了核武器冷冻运动组织举行的会议。齐默尔曼决定留下来在家乡作战而不是离开美国。他成为了一名激进的反核战斗士，他因分发传单，在内华达核试验基地被捕。和他一起的还有卡尔·萨根和400个其他的反对者。

随着东西方紧张关系的缓和，齐默尔曼的担心开始减少了，但他对政治活动的热情不减。他只是转向了另一个方向。他开始注意数字革命和加密的必要：

> 密码术一直是一种无名的科学，跟日常生活没有多大关系。在历史上，它在军队和外交通讯中扮演着特殊的角色。但到了信息时代，密码术是则关系到政治力量，

> 而且特别关系到政府和它的人民的关系。密码术跟隐私的权利有关；跟言论自由和政治联盟自由有关；跟出版自由有关；跟不被无理侵扰的自由和孤独的自由有关。

这种观点是有点偏执，但据齐默尔曼说，数字通讯和传统通讯有着一个基本的区别，这对于安全有着重要的意义：

> 在过去，如果一个政府想干涉一个公民的隐私，它需要花上相当一笔钱和力气去截获信件并阅读它们，或者窃听电话。这就和钓鱼类似，每次只能钓一条鱼。对自由和民主而言，这是非常幸运的，这种费时费力的监视在大范围内运用是不实际的。今天，电子邮件逐渐替代了邮件的角色，不久，每个人都会用它了。不像纸张邮件，电子邮件是很容易窃取的，而且只需搜索关键词就可以确定邮件内容，从而可以非常方便地、常规地、自动地甚至大规模的执行搜索。这好比是用网打鱼，一撒网，就是一片。

传统邮件和电子邮件的区别可以用下面的类比来说明。试想，艾丽丝要举办一个生日聚会，她发出了许多邀请。而伊芙，她没有接到邀请，但她想知道聚会的时间和地点。如果艾丽丝用传统的邮件方式发出邀请，那么，伊芙是很难截获邮件的。首先，伊芙不知道艾丽丝的邀请从哪儿进入邮政系统，因为艾丽丝可以用城中的任何一个邮箱。伊芙惟一截获邮件的希望是知道艾丽丝朋友的地址，从当地分发信件的邮政局中窃取信件。她必须仔细检查手中的每一封信件。如果她找到了一封艾丽丝寄的信，她要小心的打开，看完后，还要把信还原成原来的样子，以免受到怀疑。

与此相比，如果艾丽丝用电子邮件的话，伊芙的工作就变得容

易得多了。因为艾丽丝发的信息会传到一个当地的服务器中，一个进入互联网的节点：如果伊芙足够聪明的话，她可以侵入到当地服务器中。而邀请中肯定含有艾丽丝的电子邮件地址，伊芙只需搜索一些含有这地址的邮件，这一切都是很简单的事。一旦一则邀请被找到，并不需要打开信封，就可以非常方便地阅读它。况且，信息可以继续传出去，并且一点被窃听的景象都没有。艾丽丝对此毫不知情，而且也没有察觉。可是，有一个方法可以阻止伊芙读信，就是加密。

全世界每天有上亿封电子信件发出，它们都很容易被截获。数字技术帮助了通讯，同时，又使得通讯容易被监控。齐默尔曼说，密码学家有义务鼓励密码术在民间的运用，从而保护个人的隐私：

> 未来的政府继承了一套非常利用于监控的技术。他们可以观察到他们的政治敌人的每一个举动，每一次金融交易，每一次通讯，每一封电子邮件，每一个电话。所有的窃听资料可以方便地通过扫描和语音识别来筛选。是使密码术从军队的阴影中走出来，来到阳光下，去拥抱大众的时候了。

从理论上讲，1977 年 RSA 的发明是这个现象的一针解毒剂，因为，它使得个人能够制造他们的私人密钥和公开密钥，这样，个人也能安全地发送信息。然而事实上，存在着一个重要的问题就是 RSA 加密的运算量要比对称密码(比如 DES)的运算量大的多。结果是，在 1980 年代，只有军队政府和大企业才有大型计算机来实施他们的 RSA。不足为怪的是，RSA 数据安全公司，也就是商业化 RSA 系统公司，主要针对这三种消费者发展他们的加密系统。

相反,齐默尔曼认为每个人都应该能够享用由 RSA 系统提供的安全加密,从而保护他们的隐私。他把他的政治热情都放在发明一种大众用的 RSA 加密系统上了。他重新回到了他的本行计算机行业,设计一种经济而又有效的产品,而且不超越个人计算机的计算能力。他还希望他的 RSA 加密系统版本有着友好的界面,使得大众在不受密码专家指导的情况下就可以给自己的信息加密了。他把他的计划称为"相当好的隐私",简称 PGP。这个名字源自于"相当好的杂货店",是大草原家乡运动发起人之一拉尔夫主持的一个齐默尔曼喜欢的广播节目。

1980 年代后期,齐默尔曼在科罗拉多的家乡工作,他逐渐发展出了他的加密软件包。他的主要目的是加快 RSA 加密系统。一般来说,艾丽丝为了给鲍勃发信,她首先得找到鲍勃的公开密钥,然后使用 RSA 加密系统用这个密钥把信息加密。相反,鲍勃用他的私人密钥把 RSA 单向函数逆转,从而把密文解密。两个过程都需要做大量的数学计算,如果信息过长的话,使用个人计算机运算加密和解密过程都需要几分钟的时间。如果艾丽丝每天要发上百条信息,她是不能忍受这个速度的。为了加快 RSA 加密系统,齐默尔曼想出了一个非常巧的方法,他把 RSA 不对称加密系统和原来的对称加密系统联合使用。传统的对称加密系统和不对称加密系统相比是同样安全的,而且运算更快,只是对称加密系统存在着密钥分发问题,密钥必须安全的从发送者手中送到接收者手中。这却是 RSA 系统能够帮忙的地方了,因为可以用 RSA 加密系统来加密对称加密系统的密钥。

齐默尔曼描绘了以下的图景。如果艾丽丝想给鲍勃发一则加密的信息,一开始,她把消息用对称密码加密系统加密。齐默尔曼建议使用一个名叫 IDEA 的加密系统,这个系统与 DES 系统很相似。为了用 IDEA 加密,艾丽丝必须选择一个密钥,为了使鲍勃能够解密,艾丽丝不得不想个办法把密钥安全地传给鲍勃。艾丽丝

可以这样解决这个问题，她找到鲍勃的 RSA 的公开密钥，然后用它来加密 IDEA 的密钥。艾丽丝总共发给了鲍勃两个东西，一个是用 IDEA 加密的密文，另一个是用 RSA 加密的 IDEA 的密钥。在另一边，鲍勃先用他的私人密钥解密得到 IDEA 的密钥，然后，再用 IDEA 的密钥去解密信息。这看起来似乎有点费解，但这样做的好处是显而易见的，要传的信息可能很长，用对称密钥密码系统加密它的速度要快的多，而 IDEA 的密钥相对来说短的多，用相对较慢的不对称密钥加密系统加密它也不费多少时间。齐默尔曼计划把 RSA 系统和 IDEA 系统都放进他的 PGP 软件包中，但友好的界面意味着用户并不需要了解这个软件工作的细节就可以使用这个软件。在很大程度上解决了速度问题以后，齐默尔曼还给 PGP 软件包加了许多友好的特征。比如说，在运用 PGP 的 RSA 部件前，艾丽丝需要产生她的公开密钥和私人密钥。密钥的产生并非小事，因为它需要找到两个大的质数。然而，艾丽丝只需胡乱动一下她的鼠标，PGP 软件就可以产生这两个密钥，鼠标的运动提供了一个随机因素，从而，保证了每个 PGP 的用户的密钥都不会重复。每个密钥都是惟一的。此后，艾丽丝只需公布公开密钥就可以了。

PGP 软件包的另一个特色是它为电子邮件提供了数字签名。一般来说，电子邮件没有任何签名，这意味着验证信件作者的真正身份是不可能的。比如说，如果艾丽丝给鲍勃发了一封情书。鲍勃很是高兴，但他能确定这是艾丽丝写的吗？说不定是可恶的伊芙写的，然后在邮件的末尾签上艾丽丝的名字。没有手迹的辨认，判断作者的身份是不可能的。试想银行收到客户发来的一封电子邮件，在电子邮件中客户要求把所有的存款转移到一个开曼岛上的私人数字银行账户。再一次，由于没有手迹可以辨认，银行怎么才能知道这电子邮件是来自这位客户呢？电子邮件可能是一个罪犯写的，而所转到的开曼岛的银行也是他的账户。为了发展在互

联网上的信誉,发展出一种可靠的数字签名是异常重要的。

PGP 的数字签名是基于维特福德·笛福和马丁·赫尔曼所发明的原则。当他们提出分开的公开密钥和私人密钥的概念时,他们意识到他们的方法除了可以解决密钥分发问题外,还可以提供一种自然的电子邮件数字签名的方法。在第六章中,我们看到公开密钥用作加密,私人密钥用作解密。事实上,这个过程可以反过来,用私人密钥加密,用公开密钥解密。之所以没有采用这种加密方法,是因为它没有提供任何安全。如果艾丽丝用她的私人密钥加密一则信息给鲍勃,每个人都可以解密,因为每个人都能得到艾丽丝的公开密钥。然而,这种方法却可以用来做作者身份认证,因为如果鲍勃能够用艾丽丝的公开密钥解密一则信息,那么这则信息肯定是用艾丽丝的私人密钥加密的。而艾丽丝是惟一拥有这个密钥的人,那么,消息就是艾丽丝发出的。

有效的方法是,如果艾丽丝想给鲍勃发一封情书,她有两种选择。或者她用鲍勃的密钥加密以保障信的隐私,或者她用她的私人密钥加密以保证作者的确定身份。然而,如果她结合了两种方法她就可以保障隐私和作者身份认证了。有许多更快捷的方法可以做到这一点,比如艾丽丝可以通过下面的方法来发送给鲍勃的情书:她先用她的私人密钥加密她的信息,然后她用鲍勃的公开密钥加密密文。我们可以这么看,这则信息有两层外壳,一层是比较脆弱的由艾丽丝的私人密钥加密的内层外壳,一层是坚固的用鲍勃的公开密钥加密的外层外壳。结果是,鲍勃是惟一能够解开密文的人,因为只有他能够知道他的私人密钥,从而打开外层外壳,鲍勃也可以用艾丽丝的公开密钥解开内层外壳。这层外壳不是用来保证信息的安全,而是用来做身份认证的。

到这个阶段,发送一则 PGP 加密的信息变得相当的复杂。IDEA 密码用来加密信息,RSA 密码来加密 IDEA 密钥,而且如果要数字签名,还需要另一次加密。然而,齐默尔曼发明的产品可以

自动地执行这一切。所以,艾丽丝和鲍勃根本不用担心 PGP 加密中的数学问题。要给鲍勃发封信,艾丽丝只需要写好电子邮件,然后在菜单上选择使用 PGP,接着,写上鲍勃的名字,PGP 就会自动的寻找鲍勃的公开密钥,接着自动进行加密剩下的步骤。而同时 PGP 也会做一些数字签名需要的技巧。至于鲍勃接到信息后,他只需要选择 PGP 选项,然后用 PGP 解密就可以了。PGP 会自动进行作者的身份认证。在 PGP 中没有任何东西是原创的。笛福和赫尔曼早就想到了数字签名,而很多其他的密码学家也采用了对称密钥密码术和不对称密钥密码术结合的方法,以加快加密速度,但齐默尔曼是第一个把这一切结合起来制造出如此运用简便的产品的人。而且这个产品可以运用在一个中等的个人计算机上。

1991 年夏天,齐默尔曼正在把 PGP 变成完美无缺的产品。只有两个问题还待解决,它们都不是技术上的问题:一个长期的问题是,PGP 的核心 RSA 系统,是个专利产品,专利局要求齐默尔曼在推出 PGP 产品前,必须得到 RSA 数据安全公司的使用 RSA 的执照。然而,齐默尔曼决定把这个问题放在一边,PGP 并非是针对公司生产的,而更加是个人的东西,他觉得他与 RSA 数据安全公司没有利益上的竞争,因此,他希望这个公司会给他免费使用 RSA 系统的执照。

一个更直接、更严重的问题是美国参议院的 1991 年反犯罪法案,其中含有这样的条款:“国会认为,当政府得到法律授权后,提供电子通讯服务的公司和电子通讯服务设备的制造者,应该保证通讯系统允许政府得到通讯内容的明文。”参议院担心数字技术的发展,比如手机等,会使执法者无法窃听电话。然而,在强迫公司产品可以被窃听的同时,这个条款威胁着所有的安全通讯。

RSA 数据安全公司、通讯工业和公民自由组织的力量迫使国会废除了这个条款。但这只是暂时能够喘口气。齐默尔曼担心迟

早政府会卷土重来,使得 PGP 这样的产品不合法。他一直想卖出 PGP,但现在他重新考虑了他的选择。他决定与其等着 PGP 被政府封杀,倒不如在此发生之前,使每个人都能用到 PGP。1991 年 6 月,他走出了冒险的一步,他叫一个朋友把 PGP 软件公布在世界性的新闻组网络系统的公告板上。PGP 只是一个软件,所以任何人都可以免费从公告板上把它下载。PGP 现在在互联网上流传开来。

开始,PGP 只是在密码学爱好者中有所影响。但不久,它就被更广泛的互联网爱好者下载。接着,计算机杂志对 PGP 作了简短的报道,后来,就是整页关于 PGP 现象的文章了。渐渐地,PGP 开始渗入到了数字世界的每一个偏远的角落。比如说,人权活动组织开始使用 PGP 来加密他们的文档,为了防止信息落入被指控人权状况特差的政府手中。齐默尔曼开始收到赞扬他发明的电子邮件。"缅甸的抵抗组织,"齐默尔曼说,"在丛林训练营用到它,他们说它的作用很大,在没有 PGP 的时候,如果文档被搜到,常常整家人都因此被逮捕、施刑甚至杀害。"在 1991 年,在叶立钦接管莫斯科政府大楼的那天,齐默尔曼收到了一封来自于拉脱维亚的电子邮件:"菲尔,我希望你知道:希望这不会发生,但如果独裁政府接管了俄罗斯,你的 PGP 将从波罗的海到远东广泛传播,将在必要时帮助民主人士。谢谢。"

正当齐默尔曼在世界各地赢得追随者的时候,在家乡美国,他成为被指责的对象。RSA 数据安全公司决定不给予齐默尔曼免费使用 RSA 系统的授权,并很气愤他们的专利被侵犯。虽然齐默尔曼发布的 PGP 是免费软件,但它其中含有公开密钥的 RSA 系统核心,所以,RSA 数据安全公司把 PGP 列为"盗版软件",专利之争持续了好几年。在这期间,齐默尔曼遇到了更大的麻烦。

1993 年 2 月,两个政府调查员拜访了齐默尔曼,在他们质问了专利之争的问题之后,他们开始就一项更严重的指控提问。这

项指控是非法出口武器。因为美国政府把加密系统指定为武器，和导弹、追击炮以及枪支一样，PGP 在没有州政府的许可下，是不允许出口的。简言之，齐默尔曼因为在互联网上发放 PGP，而被指控非法出口武器。在其后的三年，齐默尔曼成为大陪审团的调查对象，受到联邦调查局的纠缠。

为大众加密吗？

对菲尔·齐默尔曼和 PGP 的调查引发了一场关于在信息时代加密的积极作用和消极作用的争论。PGP 的传播激发了密码学家、政客、公民自由战士和法律执行者认真思考广泛传播加密技术的意义。一些人，比如齐默尔曼，认为广泛使用加密技术是对社会有利的，因为它能保证个人在他们的通讯中有隐私权。那些反对他们的人则认为加密对社会是一种威胁，因为犯罪分子和恐怖分子可以利用它来作安全的通讯。

这场争论持续了整个 90 年代，而且现在仍继续。基本的问题是政府是否可以立法反对密码术。密码术的自由使用可以使每个人以及罪犯能够确信他们的电子邮件是安全的。另一方面，限制密码术的使用允许警方能够监视罪犯，但这使得警方也能够监视其他的守法公民。最终，我们可以通过我们选举的政府决定密码学未来的角色。这一节我们将讨论这场争论的双方的观点。许多讨论参照了美国的警方和政策制定人言论。一方面因为美国是 PGP 的故乡，所以美国成了争论的中心，另一方面，因为无论美国采取什么政策，其影响都会波及全世界。

反对广泛使用密码术的人主要是执法者，他们希望维持现状。几十年来，世界各地的警察通过合法的窃听来捕捉罪犯。比如说，1918 年的美国，用窃听消除战争间谍，到了 20 年代，它用来指证

走私犯，而且非常有效。窃听到了 60 年代成为执法者必备的工具，其时，联邦调查局意识到有组织的犯罪成为国家安全的一大威胁。执法者很难证明嫌犯有罪，因为谁要出来作证，谁就会受到暴徒的威胁，而且有可能拒绝作证的法规。警方感到他们惟一的希望是通过窃听来搜集证据，最高法院非常同意这个争辩。在 1967 年，最高法院规定只要警方得到法院的同意，就可以进行窃听。

20 年后，联邦调查局仍然认为"法院指定的电话通讯窃听是法律执行者对付贩毒、恐怖活动、暴力犯罪、间谍和集团组织犯罪的惟一有效的调查方法。"然而，如果犯罪分子使用了加密系统的话，警方的窃听会变得毫无用处。一个通过数据线的电话不过是一串数字，而且同样可以用加密电子邮件的方法来加密它。比如说 PGP 电话，是一种可以通过加密互联网传播的声音产品。

执法者争辩道：有效的电话窃听是维持法律和秩序所必需的，而加密技术应该受到限制以便他们继续他们的侦听。警方已经遇上了使用强大密码保护自己的罪犯了。一位德国的犯罪专家说："许多像贩毒和军火走私这样的不法交易已经不用电话联络了，而是通过在互联网上互发加密信息来完成交易。"一位白宫官员指出在美国也有类似的令人担忧的趋势，他声称"犯罪组织成员是一些计算机和强大密码术的高级用户"。比如说，卡利联盟就使用加密通讯来安排它的毒品交易。执法者担心互联网和密码术的联合会帮助犯罪分子联络、协调他们的力量，而他们尤其担心的是被称为"四害"的毒贩、犯罪组织、恐怖分子和贩卖儿童者将成为加密的最大受益者。

除了加密通讯外，犯罪分子和恐怖分子也加密他们的计划和记录，以防止证据的发现。奥姆真理教在 1995 年用毒气袭击了东京的地铁，他们就是用 RSA 系统加密他们的文件的。拉姆齐·尤舍弗，一位参与了世界贸易中心爆炸事件的恐怖分子，在他的笔记本电脑中保留着加密的未来恐怖活动的计划。除了国际恐怖组织

外，许多一般的罪犯也受益于密码术。比如说，一个美国的非法赌博集团也用加密法加密他们的客户，长达 4 年的时间。1997 年，由国家战略信息中心工作组授权，多里斯·德林和威廉姆·博夫进行的犯罪调查，估计有 500 起犯罪事件牵涉到了密码术，而且这个数字可能会以每年翻一倍的速度增长。

除了国内事务外，密码术也牵涉到了国家安全问题。美国国家安全局负责搜集国家敌人的情报，并破译出来。国家安全局有一个国际合作的监听网络，其中包括跟许多国家的合作，这其中包括英国、澳大利亚、加拿大和新西兰，它们共享搜到的信息。这个网络包括了许多站点，比如说在约克郡的孟威斯山信号情报基地，它是世界最大的谍报基地。孟威斯山的一部分工作牵涉到了"埃斯农"系统，它能够通过寻找特殊词汇的方式来检查电子邮件、电传和电话。"埃斯农"根据一本词典，对一些"值得怀疑的用词"，比如真主党、刺杀、克林顿，这个系统能够即时地识别出这些词。埃斯农可以对这些信件加上记号以便进一步的检查，使它能够监控来自特殊政党和恐怖组织的信件。然而，如果所有的信息是加密了的，那么，"埃斯农"就没那么有效了。参加"埃斯农"的国家就会失去宝贵的关于政治阴谋和恐怖活动的情报。

争论的另一方是公民自由战士，包括一些诸如民主技术中心和电子前线基金会这样的组织。他们支持加密公众化是因为他们坚信隐私权是一项基本的人权。就像人权宣言中第十二条中所说的："不能任意干涉任何人的隐私、家庭和住宅，也不能攻击他的声誉。每个人都要受到法律保护防止这种攻击的权利。"

公民自由战士争辩道，广泛使用加密技术是保证公民隐私权的关键。否则，他们担心未来的数字技术会使得监控变得异常容易，从而进入一个大范围窃听的时代，而且紧接着就是这种窃听的滥用。在过去，政府常常利用他们的权力窃听无辜公民的电话。总统约翰逊和总统尼克松就曾非法窃听，总统肯尼迪在他执政的

第一个月中，也进行了不清不白的窃听。在酝酿关于多米尼加进口白糖的法案时，肯尼迪在几个参议员家中安了窃听器，其理由是他相信他们收了贿赂，这似乎关系到了国家安全，可是，并没有找到任何贿赂的证据，窃听只是给肯尼迪提供了有利的政治情报，使他成功通过了这个法案。

最出名的非正义窃听事件之一是关于马丁·路德·金的。他的电话被监听了好几年。比如说，1963 年，联邦调查局通过窃听得到金的信息，并把这个信息告诉了参议员詹姆斯·伊斯特兰德，为的是让这位参议员能够在一项人权法案的争论上有利。更有甚者，联邦调查局搜集金的个人生活细节，为的是诋毁他的声誉。录有金讲的黄色笑话的磁带被送到他的妻子手中，而且在约翰逊总统面前播放。然后，在金取得诺贝尔奖后，关于金的生活上令人尴尬的细节被送到任何一个想授予金荣誉的组织手中。

其他政府也同样滥用监听手段。法国估计大约每年有将近 10 万次非法的窃听。而且可能最为侵犯公民隐私权的就是"埃斯农"系统了。"埃斯农"并不判断它的监听的合法性，它并不是针对某个人的监听，相反，它不加选择地搜集信息，用接收器接收卫星的通讯。如果艾丽丝给鲍勃发了一封没有恶意的跨洋电子邮件，它无疑会被"埃斯农"所截获；而如果这封信中恰巧含有几个"埃斯农"词库里的单词，它就会被打上标记，同极端组织和恐怖组织的信件一起作下一步的检查。一方面执法者认为加密是应该被禁止的，因为这样会使"埃斯农"无效；而另一方面公民自由战士却认为正因为加密能使"埃斯农"无效，所以，才要普及加密术。

当执法者争辩说加密会减少犯罪的指证，公民自由战士的回答是隐私权是更为重要的。无论如何，公民自由战士强调加密并非是执法的重要障碍，因为在大多数案件中，窃听并没有扮演重要角色。举例说明，1994 年美国法院批准了近 1000 次窃听，和总共发生的 25 万个案件相比，这个数目就微不足道了。

不足为奇,在密码术自由的拥护者中有一些公开密钥密码术的发明人。笛福声称大多数历史上个人享有完全的隐私权:"在18世纪90年代,权利法案得到认可,任何两个人都可以进行一次完全隐私的对话,他们只需看看四周是否有人就可以了,这是现在的人没法享有的。当时,没有录音设备、麦克风和激光干涉机等。你会记录到这个文明仍然尚存。我们大多数人认为那是美国政治的黄金时期。"

罗·里维斯特,RSA的发明人之一,认为限制密码术的使用时是愚蠢的:"只因为一种科技可能被犯罪分子所利用,就不分青红皂白地取缔它,这种做法是非常愚蠢的。比如说,任何美国公民都可以自由地买到一副手套,而抢劫犯也可以利用它在入室抢劫不留下指纹。密码术是一种数据保护的科技,这和手套相似,手套是用来保护手的科技。密码术可以保护数据不受黑客和间谍的侵犯,而手套则保护手不被切伤、擦伤、烫伤、冻伤和感染。前者使联邦调查局不能够窃听,后者使联邦调查局的指纹分析术不能运用。密码术和手套同样的便宜,都很容易得到。事实上,你从互联网上下载密码软件的钱要比买一副好手套的钱少得多。"

公民自由战士的最大可能联盟是大公司。电子商务刚刚起步,但发展速度非常快。以图书、音乐CD和计算机软件的零售业作为先锋,超市、旅行社和其他的商务紧接其后。1998年,英国人通过互联网买的产品总数超过4亿英镑,到了1999年,这个数字翻了4倍。几年后,互联网上的商业将统治整个市场,除非商业遇上了安全和信任的问题。一个企业必须能够保证金融交易的隐秘和安全,而惟一的方法就是使用强大的密码术。

此刻,互联网上的交易可以用公开密钥密码术来保证安全。艾丽丝拜访一个公司的网站,选择要买的产品,填好一张表格,其中有她的名字地址和信用卡等内容。艾丽丝用公司的公开密钥加密这个表格,然后传给这个公司。这个公司可以解密这个信息,因

为只有他们有私人密钥。这一切都自动在艾丽丝的浏览器上完成,这时浏览器与公司的计算机相连。

通常,加密的安全取决于密钥的长度。在美国对密钥的长度没有任何限制,但美国软件公司仍不准出口含有强大密码术的网络产品。因此,出口到其他国家的浏览器只能用长度较短的密钥,因此只能得到中度的安全保证。实际上,如果艾丽丝在伦敦买一本芝加哥公司的书,而鲍勃在纽约向同一家公司购买一本书,艾丽丝的互联网交易要比鲍勃不安全千百万倍。鲍勃的交易是完全安全的,因为他的浏览器支持大数字的密钥加密,而艾丽丝的交易可能会被恶意的罪犯破解。幸运的是,破解艾丽丝信用卡所用设备的价格远远比它的最高金额限制要高得多,所以这样的破译是不值得的。然而,随着互联网上的交易金额的增长,最终,破解信用卡将会成为有利可图的事情。简言之,如果互联网贸易兴起,世界各地的消费者必须有相当的安全保证,而且大公司也不能容忍被削弱的加密。

公司需要强大密码还有另一个原因。公司储藏着大量的信息和计算机数据,包括产品的描述、客户资料和商业账目。很自然,公司需要保护这些信息,以防黑客侵人计算机后把信息偷走。这种保护可以通过加密信息的方式进行,这样只有拥有密钥的雇员才能取得这资料。

概括一下总的状况,很明显这是两个阵营的争论:公民自由战士和商家是支持普及强大密码术的,而执法者则希望限制普及强大密码术。总的来说,公众的观点是支持前者的。这部分原因归功于几部好莱坞的电影。在 1998 年早期,《水星的升起》讲述了一个患孤僻症的 9 岁孩子,无意中破解了国家安全局的密码。国家安全局派出了亚力克·鲍德温,一位国家安全局的雇员,去刺杀这个被视为是威胁国家安全的小孩。幸而,这个小孩有布鲁斯·威利斯保护。也是在 1998 年,好莱坞放映了《国家的敌人》。这个影片

讲的是国家安全局刺杀了一位支持强大密码术议案的议员。这位政客被刺杀了,但威尔·史密斯所饰的律师和吉恩·哈克曼所饰的前国安局的雇员,最终把国家安全局送上了正义的审判。两部电影都把国家安全局描述的比中央情报局更罪恶。在许多方面,国家安全局扮演了潜在威胁的角色。

然而,除了密码术自由的支持者和限制密码术的支持者,还有第三种意见,这个意见提出了前两种意见的折衷方案。在过去的10年中,密码学家和政策制定人一直调查一个名叫"第三方掌管密钥"的方案。术语"第三方掌管"的意思是甲方把钱交给第三方,第三方在特定的条件满足后,把钱再交给乙方。比如说,租房人把一笔保证金放在律师那儿,在房屋发生损坏的情况下,律师可以把这笔钱交给房主。在密码术中,艾丽丝要给第三方她的私人密钥的拷贝,第三方是独立可靠的中间人。如果有足够证据说明艾丽丝卷入了犯罪,第三方有权把艾丽丝的私人密钥交给警方。

这种方法最出名的一次尝试是于1994年采纳的美国第三方加密术标准。其目标是为了鼓励使用两种加密系统,称为"大剪刀"和"压顶石",它们分别用来加密电话通讯和计算机通讯。要用大剪刀密码,艾丽丝必须先买一部预装了芯片的特殊电话,芯片中有她的私人密钥。就在她买这部电话的同时,芯片中密钥的副本被分成两部分,每一部分送给两个不同的联邦权利机关用来保存。美国政府争辩说艾丽丝是有安全保证的,她的密钥只有在执法者说服两个权力机关,证明她有案在身的情况下才会泄露给执法者。

美国政府在它们自己的通讯中运用"大剪刀"和"压顶石"加密,使得与政府打交道的公司也不得不采用这种加密。其他企业和个人则可以自由运用任何加密方法,但政府希望"大剪刀"和"压顶石"加密普及起来,成为整个国家最流行的加密系统。但事实不是这样,第三方密钥没有赢得多少支持者。公民自由战士并不喜欢联邦权利机关掌握着每个人的密钥——他们做了一个类比,把

密钥比作真正的钥匙，问人们是否希望政府有我们屋子的钥匙？密码学专家指出，一个骗子雇员通过高价买密钥的方式就可以摧毁整个密码系统。企业当然对此非常担心。比如，一个在美国的欧洲企业就会担心它们的通讯被美国政府截获，使美国的竞争对手受益。

虽然“大剪刀”和“压顶石”失败了，但许多政府仍然相信第三方密钥方案是可行的，条件是只要保证罪犯不可能窃取到密钥，只要向公民再次保证政府不可能滥用密钥。1996 年联邦调查局主管路易斯·J·福里如是说：“执法的社团全力支持一种折衷的加密政策……第三方密钥也许不是惟一的解决方案，但它实际上是一个非常好的方案。因为它有效地平衡了主要社会的隐私权、信息安全、电子商务、公众安全和国家安全。”美国政府支持它的第三方密钥提议，许多人怀疑它在未来会变着形式再次推销它的第三方密钥。在目睹选择性的第三方密钥失败后，政府甚至会考虑强迫用第三方密钥。而同时，密码术自由的支持者们继续反对第三方密钥。一位技术记者肯尼斯·内尔·库科尔写道：“卷入密码术之争的人们是聪明的、高尚的或者是拥护第三方密钥的，但他们最多同时具有以上所说的两点。”为了平衡公民自由权、商业以及执法，政府还可以选择许多其他的方法。要说哪一种是最好的选择似乎还很遥远，因为现在的密码政策飘忽不定，一系列的世界事件都影响着关于密码的争论。1998 年 11 月，英国女皇的讲话宣布了英国的数字市场加密合法化的时代到来。1998 年 12 月，33 个国家签署了瓦参奈尔协议，限制了武器出口，其中包括强大密码术。1999 年 1 月，法国迫于商界的压力撤销了反密码术的法律，这项法律原来在西欧是非常严格的。1999 年 3 月，英国政府发表了一个关于电子商务货币的咨询文件。

等你读到这本书时，关于密码术政策的争论肯定又有几个来回了。然而，未来密码术的政策有一点是可以肯定的，就是身份验

证。如果艾丽丝需要给一个新朋友泽克写封安全的信,她需要知道泽克的公开密钥。她可能会通过电子邮件向泽克询问他的密钥,叫他把他的密钥通过电子邮件传给她。不幸的是,如果伊芙截获了泽克的回信,她可能毁掉它,然后伪造一封回信给艾丽丝,其中不是泽克的密钥而是伊芙她自己的密钥。艾丽丝就会把一封重要的信件用伊芙的密钥加密后发给泽克,这一点她却毫不知情。如果伊芙截获了这封重要的邮件,她就很容易解密并阅读它了。换言之,公开密钥密码术的问题之一是怎么确信你用的公开密钥就是你想要通讯的对方的密钥呢?认证权威机构是用来检验公开密钥和其主人的对应关系的组织。一个认证权威机构可能会请泽克来面对面确定他的公开密钥。如果艾丽丝相信认证权威机构的话,她可以通过这个机构获取泽克的公开密钥。

我已经讲过艾丽丝怎样从网上向公司购物,填写表格,并用那家公司的密钥加密。事实上,她在做这以前必须先确定一件事,她必须确信这个密钥是被公证过的。1998年,权威认证市场的先行者维力珊公司在仅仅四年的时间内就成为了价值3000万美元的大公司。除了保证公开密钥的正确性外,权威认证机构必须也保证数字签名的准确性。1998年,爱尔兰的巴尔的摩技术公司提供了美国总统克林顿和首相亚亨的数字签名的确认。这使得两国领导人可以在都柏林用数字签名签署公报。

权威认证机构对安全通讯没有威胁。它们只是让泽克公布他的公开密钥,使其他想给泽克写信的人可以确认这是他的密钥。然而,还有其他种类的公司,被称为第三信任方(简称 TTP)提供一种更受争议的服务,这种服务叫做密钥恢复。试想一个法律公司把它的所有重要的机密都用它的公开密钥加密了,以防止被黑客或其他一切可能想要这资料的人偷窃。然而,如果藏有私人密钥的雇员把它给忘了,或者这个雇员潜逃了,抑或被公共汽车撞死了呢?政府鼓励像 TTP 这样的机构保存所有的私人密钥。一个

公司如果把私人密钥丢了,它可以通过 TTP 恢复。

第三信任方是有争议的,因为它们可能掌管着人们的输入密钥,因此它们有能力阅读他们客户的信息。它们必须是十分让人信任的,否则,这个系统很容易被滥用。一些人争辩道,TTP 是第三方密钥的替代品,在做调查时,执法者可能使 TTP 屈服,交出它们客户的密钥。其他人则认为 TTP 是公开密钥密码术不可或缺的一个组成。

没有人能够预测 TTP 将来会扮演什么角色,也没有人能猜到 10 年后密码术政策会是什么样子,然而,我觉得在不久的将来,支持密码术广泛使用的人会赢得这场争论。因为没有哪个国家希望加密的法律阻止电子商务的发展,然而,如果结果证明法律是错的,总是有机会修改法律的。如果有一系列的恐怖活动,而执法者证明窃听确实有助于制止恐怖活动,那么政府会立即赞同第三方密钥的政策,所有强大密码术的用户会被强制放弃原来的密码术,使用第三方密钥的密码术,此后,用发送其他强大密码术加密的信息将被视为违法。如果对这种行为的惩罚十分严厉,执法者又占了上风,接着,如果政府滥用第三方密钥,公众又会重新倡导密码自由,局势又开始逆转。简而言之,我们没有理由不根据环境调整我们对政策的看法,以适应当时的政治、经济和社会风气。这一切的决定因素是两个公众最害怕的东西——政府和罪犯。

齐默尔曼的复原

1993 年,菲尔·齐默尔曼成了大陪审团的调查对象。根据联邦调查局所说,他非法出口军火,因为他给敌对国家和恐怖分子提供了进攻美国政府的工具。随着调查的进行,越来越多的密码学家和公民自由战士加入了支援齐默尔曼的行列,他们成立了一个

国际基金会来负担齐默尔曼的律师费用。同时，因为受到联邦调查局的调查，PGP 的声名大振，齐默尔曼的发明以更快的速度在互联网上传播——毕竟，这可是连联邦调查局都害怕的加密软件。

"相当好的隐私"公布时非常仓促，这使得它还没来得及作最后的修饰和完美化。不久，就有要发展一个更完美的版本的 PGP 的呼声，但显然齐默尔曼没法再继续他的工作了。一群欧洲的软件工程师接替了他的工作，重新建造更完美的 PGP。总的说来，欧洲对密码的态度一直比较放松，没有出口欧洲版 PGP 的禁令，而且 RSA 专利问题在欧洲也不存在，因为 RSA 专利没有在美国以外的国家申请。

经过三年的大陪审团调查，仍没有把齐默尔曼送上法庭。这个案件因为 PGP 的特性和它的发放方式变得异常复杂。如果齐默尔曼把 PGP 装在一台电脑中，然后把电脑运到一个敌国，那么他肯定处于及其不利的位置，因为他显然把一个可用的密码系统出口到国外。类似的，如果他出口了一张含有 PGP 的磁盘，这张磁盘就会被认为是密码术设备，而证明齐默尔曼有罪的证据就相当确凿了。另一方面，如果他把他的程序印在书上，把书带到国外的话，那他被视为是出口一种知识而非密码术设备。然而，书上的程序可以用扫描的方法转换成电子符号，成为计算机可以用的程序，这意味着书和磁盘是一样危险的。而事实上，齐默尔曼只是碰巧把一个 PGP 程序的副本给了一个朋友，这个朋友只是把它安装在一台美国的计算机上，而碰巧的是这台计算机连着互联网，此后，一个敌国可能也可能不会下载它。齐默尔曼真的犯有"出口 PGP"的罪吗？直至今天，这个关于互联网上的法律问题一直在不断地讨论和诠释。在 90 年代初，这个问题就更模糊了。

1996 年，经过 3 年的调查后，美国律师总部放弃了针对齐默尔曼的案件。联邦调查局意识到已经太晚了——PGP 早已逃入了互联网，起诉齐默尔曼不会有任何好处。还有一个重要的问题

是齐默尔曼受到了许多大机构的支持,比如麻省理工学院出版社,它出版了关于 PGP 的 600 页的书,这本书散发到世界各地。所以,起诉齐默尔曼等于起诉麻省理工学院出版社。联邦调查局不愿意起诉的另一个原因是,齐默尔曼很可能被判无罪,联邦调查局的起诉不会得到任何好处,相反,它会引起一场关于隐私权的宪法的争论,大众也会同意广泛使用密码术。

齐默尔曼的其他问题也一同消失了。他从 RSA 公司那儿取得了使用 RSA 系统的执照,从而解决了专利问题。最终,PGP 成了合法的产品,而齐默尔曼也是个自由人。这次调查使他成为密码的改革者,世界上任何一位市场经理都会羡慕 PGP 得到的免费宣传。1997 年年末,齐默尔曼把 PGP 卖给了网络联盟,自己成为它的一位资深人员。虽然 PGP 现在卖给公司,但它对不做商业目的,使用加密仍然是免费的。换言之,任何想保护他的隐私权的个人,可以在互联网上免费的下载 PGP。

如果你也想得到 PGP,有许多的网站提供下载服务,你可以很容易地找到它们。可能最为权威的网站是 http://www.pgpi.com/,PGP 的主页,在那儿你可以下载 PGP 的美国版和国际版。在这里,我不想对你使用 PGP 负任何责任。如果你选择使用 PGP,是由你决定你的计算机是否可以运行它,软件是否染毒等等。而且,你应该检查一下你所在的国家对使用强大密码术的规定。最后,你应该确定该下载什么版本的 PGP:生活在美国以外的个人不能够下载美国版本的 PGP ,因为这违反了美国出口的法律。PGP 的国际版则不受出口禁令的限制。

我仍然记得我第一次下载 PGP 的那个星期天的下午。从那以后,我能保证我的电子邮件不会被截获和阅读,因此我可以给艾丽丝、鲍勃或任何其他拥有 PGP 的人发送加密的重要文件。我的笔记本电脑和 PGP 软件给我提供的加密,是世界上所有解密设备加起来都无法破解的。这使我心满意足。

第八章 量子的飞跃

两千年来,密码制造者和密码破解者一直在战斗,密码制造者保藏秘密,密码破解者竭尽全力地破解秘密。这一直是一场旗鼓相当的战斗,当先前的方法不再安全时,密码制造者就发明新的、更有效的加密术。密码制造者似乎领先了,但密码破解者马上就会反击。公开密钥密码术的发明,以及政府之间围绕强大密码术在民间使用的争论,到今天,很明显,密码学家赢得了这场信息战争。菲尔·齐默尔曼总结说,我们正生活在密码术的黄金时代,他说:"现在,用现代密码术制造的密码,很可能已经远远超出了所有已知密码破译术能破解的范围。而且,我认为,这种情况会一直存在下去。"齐默尔曼的观点得到了在国家安全局任职的威廉姆·科洛维尔和德比特·德里科特的认同,他们说:"如果让全世界将近260 000 000台个人电脑一起来破解一个简单的PGP加密的信息,这个工作平均要花大约12 000 000倍宇宙年龄的时间来完成。"

但不管怎样,以前的经验告诉我们,每一个号称是不可破解的密码,迟早都会"屈服"于密码破译术。维热纳尔密码被称为"不可破译的密码",但被巴比奇破解了;恩格玛机曾一度被誉为是无懈可击的,直到保罗斯发现了它的弱点。那么,到底是密码破解专家

找到了另一个突破口，还是齐默尔曼的结论是正确的呢？预言任何一项技术未来的发展状况总是不可靠的，预言密码的发展更是极其冒险的。我们不仅必须猜测哪一个发现会跟未来有关，而且还必须猜测哪一项发明跟现在有关。詹姆斯·埃利斯和政府通讯总部的故事使我们引以为戒，也许早已有明显的破绽就隐藏在政府掩盖的秘密背后。

在最后一章中，分析了一些可能在21世纪增强或破坏保密性的未来派的想法。下一部分着眼于展望密码破译术的未来，特别是其中的一个想法可能使密码破解专家能破解现在的所有密码。另一方面，本书的最后一部分展现了一个最使人兴奋的密码学的前景，一种有潜力的能绝对保证保密性的系统。

密码破译术的未来

不论是实力强大的RSA实验室，还是其他的现代密码专家和密码破解专家都仍然能在情报收集中扮演很重要的角色。事实证明了他们的成功，即密码学家的需求量比以前多得多——国家安全局仍然是世界上雇佣数学家最多的单位。

在地球上传播的信息中只有一小部分是被安全地加密了的，剩下的信息要么是拙劣地加密，要么根本不加密。这是因为互联网的用户数量增加很快，然而这些人中极少有人在保密性方面采取足够的防范措施。这样就会造成国家的安全部门、执法者，抑或任何一个有好奇心的人都可以把他们的魔爪伸向他们不该拥有的信息。

甚至即使用户正确使用了RSA提供的密码，仍会有很多密码破解者能从截获的消息中收集到信息。密码破解者继续使用像交换分析这样的旧式技术；如果密码破解者不能彻底了解一个信息

的内容,那他们至少可能找出是谁发的信息,谁会接到这条信息,而信息本身就会泄密。密码破解术最新近的发展被称为“暴风雨攻击”,其目的是要用计算机的显示器来显示侦查到的电子装置发出的电磁信号。如果伊芙将一辆有蓬货车停在艾丽丝家的外面,她就能用灵敏的“暴风雨”仪器来分辨艾丽丝在电脑上设定的每一个单独的按键。这就使伊芙能截获敲进电脑中的,还没有加密的信息。为了抵抗“暴风雨攻击”,一些公司已经推出起防护作用的材料,将其用在屋子的墙上就能阻止电磁信号的外泄。在美国,必须取得政府的许可才能购买这种防护材料,这就暗示一些组织比如像联邦调查局,一般是依靠“暴风雨”进行监视的。

其他的攻击方式包括使用病毒和“特洛伊木马”。伊芙可以设计一个电脑病毒感染 PGP 软件,这个病毒就被静悄悄地带进了艾丽丝的电脑中。当艾丽丝使用她的私人密钥解密一个信息时,这个病毒就会运行,并把这个密钥记录下来。接下来的时间,艾丽丝登陆互联网,病毒秘密地将这个私人密钥传给伊芙,这样伊芙就能把以后艾丽丝收到的所有信息解密。“特洛伊木马”是另一种软件“骗术”,就如同伊芙设计了一个程序,表面上看很像真正的加密工具产品,但实际上它泄漏用户的密码。艾丽丝会相信自己下载了一个可信的 PGP 复本,然而她真正下载的是“特洛伊木马”的伪装版本。这个修改的版本看上去就像真正的 PGP 程序,但其中含有将艾丽丝的所有通信的明文复本发给伊芙的指令。正如菲尔·齐默尔曼指出的:“任何人都能修改源代码,然后制造出一个像真的 PGP 程序的‘行尸走肉’,执行它魔鬼主人的命令。这个伪装成 PGP 的‘特洛伊木马’版本能被广泛传播,并声称是从我这儿传出去的,多么阴险啊!不管采取什么方法,你都应该尽力从一个可靠的来源获得 PGP。”

改动的“特洛伊木马”引用的是新编的、看上去很安全的加密软件的一部分程序,但实际上这部分程序含有一个“后门”,它使它

的设计者可以把每一个人的信息解密。在 1998 年,韦恩·麦德森的报道中,揭露了瑞士的一家密码公司 Crypto AG 在其产品中设置了“后门”,而且还将“后门”的具体使用方法提供给了美国政府。也就是说,美国可以读取一些国家的通讯。1991 年,刺杀流亡的前伊朗首相的刺客在被捕时说,他很感谢 Crypto AG 公司的帮助使他窃听到伊朗信件的译本。

尽管交换分析,“暴风雨攻击”、电脑病毒和“特洛伊木马”都是收集情报的有用技术,但是密码学家认识到,他们真正的目的是找到一种好的方法破解被称为现代加密术基石的 RSA 密码。RSA 密码被用于保护非常重要的军事上的、外交方面的和犯罪分子之间的通讯——确切地说,这些信息都是情报收集部门想要译解的。如果密码学家向强大的 RSA 密码挑战的话,他们需要找到较好的理论或技术上的突破。

理论上的突破将是获得艾丽丝私人密钥的新方法的基础。艾丽丝的私人密钥是由 p 和 q 组成的,它们是公开密钥 N 选择质因数分解得到的。标准的方法是逐个检查每个质数看它是否能整除 N,但我们知道这将花费大量的时间来完成。密码学家竭力要找到一条质因数分解的捷径,以寄希望这种方法能极大地减少分解得到 p 和 q 所要求的步骤,但迄今为止,所有为完善质因数分解方法的努力都以失败而告终。几个世纪以来,数学家们一直在研究质因数分解,但现代的质因数分解方法并不比古代的方法有效多少。当然,很可能是由于数学的相关特性就注定了质因数分解捷径是不存在的。

在理论上密码学家认识到寻求突破不会有太大的希望,他们不得不从技术方面着手创新。如果没有什么显著的方法减少质因数分解所需要的步骤,那么密码学家就需要一种能更快完成这些步骤的技术。虽然硅片的速度大约每十八个月就会增长两倍,而且今后还会更快,但是这不足以在加快质因数分解的速度上造成

真正的影响——密码学家需要一种比现在的计算机快几百万倍的技术。因此，密码学家期待着一种彻底的新式计算机——量子计算机的问世。如果科学家能造出一台量子计算机的话，那它将能以超常的速度进行计算，这种速度使现代的超型计算机看起来像是一个坏了的算盘。

在本节接下来的部分中讨论的是量子计算机的概念，因此，将要涉及一些量子物理有时也称量子力学的原理。在深入讲述之前，请记住量子力学的创始人之一尼尔斯·波尔的"警告"："如果一个人读量子力学时不感到吃惊，那他就是没有理解量子力学。"换一句话说，作好思想准备去面对一些很令人晕头转向的理论。

要说明量子计算机的原理，则应追溯到18世纪末托马斯·杨的工作。托马斯·杨是英国的博学者，他最先破译了埃及的象形文字。在剑桥的以马内利学院读书时，杨经常在学院附近的鸭子池塘度过下午的休闲时光。一个普通的日子因为一件事情的发生而变得非同寻常。这一天，杨注意到两只鸭子互相并排着在一起快乐地游泳。他观察到两只鸭子在身后留下了两道水纹，这两道水纹相互作用形成了一种特殊的凹凸和水平状斑点相间的水纹。这两道水纹在鸭子身后扇状分布，并且当一只鸭子发出的波峰碰到从另一只鸭子发出的波谷时，其结果是形成水平面的小斑点——也就是波峰和波谷互相抵消了。另一种情况，如果两个波峰同时到达同一点，则形成一个更高的波峰。而如果是两个波谷同时到达同一点，则形成一个更深的波谷。杨被深深地吸引住了，因为这个现象让他回想起他在1799年做的一个关于自然光的试验。

杨在较早时做了这样一个试验，他在一个隔板后设置了一个光源，在隔板上有两个细窄的竖直狭缝，如图71(a)所示。杨又在离隔板一定距离的地方放了一块屏幕，让从两个狭缝穿过的光波投射在上面以便观察。光源打开后，他发现从两狭缝射出的光呈扇状分布，而后在屏幕上形成了明暗相间的光斑。这些光斑让杨

感到很迷惑，但现在他相信，根据在鸭塘看到的景象他能完全解释为什么会出现这种现象。

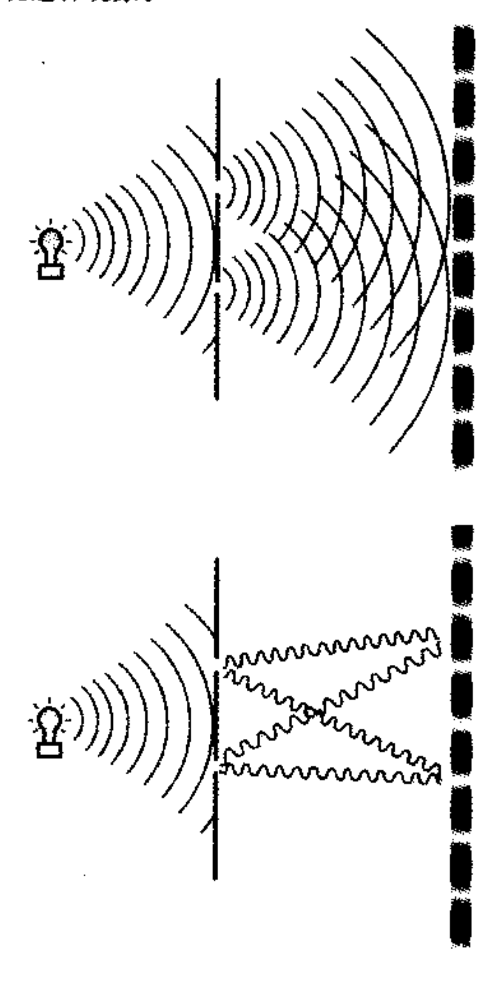


图 71：杨傲的光的衍射实验

杨开始设想光是以波的形式存在的。如果从两个狭缝发出的光有波的特征,那么它就会和两只鸭子身后的水波一样具有同样的性质。这就意味着,在屏幕上出现的明暗相间的光斑的成因,也就类似于水纹之间的相互作用导致形成的高峰、低谷和水平的斑点。杨想像到在屏幕上是暗斑的点是光波谷碰到光波峰,二者相互抵消的结果;而在屏幕上形成明斑的点则是两个光波峰(或两个光波谷)相遇,彼此增强的结果,如图 71(b)所示。鸭子使杨更加深入地认识了真实的自然光,最后他出版了《光的波动理论》这部空前的物理杰作。

今天,我们知道光确实是一种波的形式,但我们也知道它同时还具有粒子的性质。光以波的形式存在还是以粒子的形式存在,视条件而定。光的这种不确定性被称为光的波粒二相性。我们没必要更深入地讨论光的二相性,但要说明的是现代的物理学思想认为一束光是由无数个独立的粒子组成的,这些粒子称为光子,光子表现波的性质。根据这个观点,我们可以这样解释杨的试验,光子穿过狭缝,在隔板的另一边发生干涉作用。迄今为止,杨的试验还没有什么特别奇异的发现。然而,现代技术已能使物理学家用一根纤维重复杨的试验,这纤维细到每次只能发出单个光子。光子以每分钟一个的速率产生,并朝着隔板的方向运动。常常就会有一个光子穿过其中的一个狭缝,打到屏幕上。虽然我们的眼睛没有那么高的灵敏度能看到这些单个的光子,但我们能借助特殊的检波器观察到它们。经过几个小时后我们就构建了一张完整的光子打在屏幕上的图。在某时若只有一个光子通过狭缝,我们并不希望看到杨观察到的光斑,因为这个现象似乎要由两个光子同时穿过不同的狭缝,在另一边产生干涉作用。相反我们希望看到的是只由隔板上的狭缝发出的两束光波产生的光斑。然而,由于一些特殊原因,甚至只有一个光子也能在屏幕上形成明暗相间的光斑,就像很多光子发生的干涉现象。

这个奇特的结果与常理相悖。这个现象无法用经典的物理理论来解释,这些创建起来的理论只适用于日常事物。经典的物理学能解释行星运行的轨道或炮弹的弹道,但却不能描述真实的微观世界,比如一个光子的轨道。为了能解释诸如光子这一类现象,物理学家借助于量子理论,它能解释物体在微观水平的运动行为。然而,就连量子理论家在怎样解释这个现象时也不能达成一致。他们渐渐分成两个意见相反的阵营,各自坚持自己的解释。第一个阵营的解释被称为"重叠理论",该理论是以我们惟一知道的关于光子可确定的两件事为前提条件,也就是光子离开纤维和它打到屏幕上。而其他的事情都是完全未知的,包括光子是从左边的狭缝穿过的还是从右边的狭缝穿过的。因为光子确切的路径不知道,所以重叠理论的支持者们得出一个特别的观点,光子以某种方式同时穿过两个狭缝,然后它自身发生干涉,在屏幕上产生观察到的光斑。但是一个光子怎么同时穿过两个狭缝的呢?

重叠理论的支持者对此做如下解释。如果我们不知道一个粒子正在做什么,那么它有条件可能在同一时间做每一件事。在这种情况下的光子,我们不知道它穿过的是左边的狭缝还是右边狭缝,所以我们假定它同时穿过了两个狭缝。每种可能性称为一种状态,因为光子满足这两种可能性,所以说它处于两种状态的重叠状态。我们知道一个光子离开纤维,我们还知道一个光子在隔板的另一边打在屏幕上,但在这其间,光子以某种方式分离成两个"鬼光子"穿过两个狭缝。重叠理论听起来可能有些可笑,但至少解释了用单个光子演示杨的试验产生的光斑结果。与此相反,旧式的经典观点是光子只能穿过其中的一个狭缝,我们只是不知道是哪一个——这感觉上比量子的观点更合乎情理,但不幸的是它不能解释观察到的结果。

在1933年获得诺贝尔物理学奖的埃尔温·薛定谔,创立了被称为"薛定谔的猫"的理论,经常被用来帮助解释重叠理论的概念。

假定在一个盒子里有一只猫。猫可能有两种状态:即要么是死的要么是活的。开始的时候,我们知道这猫确切地处于一种特殊的状态,因为我们能看见它是活的。在这个时候,猫不存在重叠状态。接下来,我们在靠近盖子的地方放入一小瓶氰化物和猫同处于盒子中。现在我们在一段时间内不知道有什么事情发生,因为我们不能看见或测量猫的状态。它还活着,还是踢破了装氰化物的瓶子死了?按照惯例我们会说猫要么活着要么死了,我们只是不知道是哪一种状况。可是,量子理论的说法是这只猫处在两种状态的重叠状态——它既是活的也是死的,它满足所有的可能性。重叠状态仅仅是在我们没有看着这个物体的时候发生的,这是一种描述处在不确定状态时的物体的方法。最后我们打开了盒子,我们就能看到猫活着还是死了。看猫的这个举动强迫猫处在了一个特殊的状态,就在这个非常时刻,重叠状态消失了。

如果有的读者不能接受重叠理论,这是第二个阵营的观点,另一种对杨的试验的解释。但不幸的是,这个观点也很怪异。这个"多元世界论"认为,离开纤维的光子有两种选择——它要么穿过左边的狭缝要么穿过右边的狭缝——在这个时刻宇宙分成了两个宇宙,在一个宇宙光子穿过的是左边的狭缝,在另一个宇宙光子穿过的是右边的狭缝。这两个宇宙以某种方式互相干涉,这就说明了光斑的形成。多元世界论的支持者相信任何时候一个物体都有进入几种可能状态中的一种状态的潜能。宇宙分成了许多宇宙,所以每一种潜能都能满足不同的宇宙。这种宇宙增殖的理论称为"多元宇宙论"。

无论我们接受的是"重叠理论"还是"多元宇宙论",量子理论都是一门令人困惑的哲学。尽管如此,它仍是至今为止所创立的科学理论中最成功、最实用的理论。包括量子理论在解释杨的干涉试验结果时独一无二的能力,它还成功地解释了许多其他的现象。只有量子理论才能使物理学家计算出发电站核反应堆反应的

后果；只有量子理论能解释 DNA 这个奇迹；只有量子理论才能解释太阳是怎样发光的；只有用量子理论才能设计出激光在立体声播放器上播放音乐。因此，不管你喜欢与否，我们都生活在一个量子的世界。

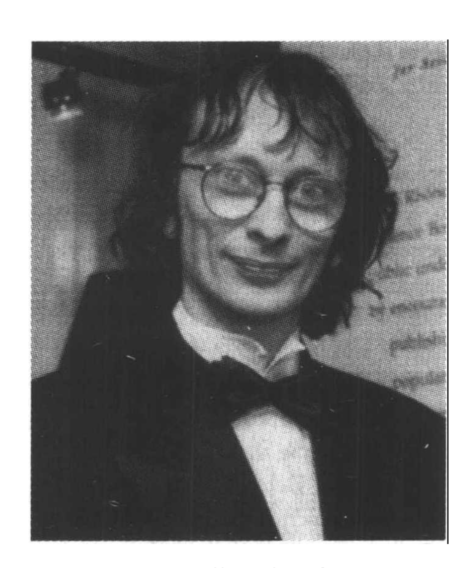


图 72：戴维·多伊奇

在所有的由量子理论推出的结论中，在技术方面最重要的就是造出量子计算机的可能性。量子计算机的出现既预示着计算能力的新时代的到来，又将破坏现代密码的安全性。英国物理学家戴维·多伊奇是研究量子计算机的先锋之一，他在 1984 年参加了一次关于计算理论的会议，之后开始着手这方面概念的工作。在这次会议中，多伊奇在听一个报告时发现有些东西以前没有注意到。公认的前提条件是所有的计算机基本上都是依据经典的物理学定律进行操作的，而多伊奇坚信计算机应该遵守量子物理的定

律，因为量子定律更基础。普通的计算机操作是在一个相对的肉眼可见的水平上，在这个水平上量子定律和经典定律几乎区别不开。因此科学家们一般都认为普通的计算机是以经典物理学为依据的，这没有什么关系。然而在微观的水平上这两套定律就会出现分歧，而且在这个水平上只有量子物理定律才掌握着真理。在微观水平，量子定律展示了其令人惊异的作用，一台计算机的构件利用这些定律将以彻底的新方式运作。会议结束后，多伊奇回到家中，开始从量子定律着手改写计算机的理论。他在1985年发表的一篇论文中描述了他设想的根据量子物理定律进行操作的量子计算机。特别的是，他阐明了他的量子计算机与普通计算机的不同点。假设你有一个问题，这个问题有两种形式。在一台普通计算机上回答这个有两种形式的问题，你不得不将第一种形式输入电脑然后等待答案，接着输入第二种形式再等待这个答案出来。换句话说就是，一台普通的计算机一次只能处理一个问题，如果有几个问题，那它只能逐个处理。但用的是一台量子计算机的话，这两个问题会被合并成两种状态的重叠态，然后同时被输入电脑，接着计算机本身将进入两种状态的重叠态，一种状态就是一个问题。或者根据“多元宇宙论”，计算机将进入两个不同的宇宙，在不同的宇宙中回答这个问题的每一种形式。不管用哪种理论，只要利用量子物理定律，量子计算机就可以同时处理两个问题。

量子计算机有多大威力，我们可以比较一下它和普通计算机在性能上的差别，看它们各自在处理一个特殊的难题时会发生什么作用。比如这一道题：找到一个数，要求它的平方和立方一共用了阿拉伯数字0到9一次而且只有一次。如果我们试一下数字19，就会发现 $19^2 = 361$；$19^3 = 6859$。19不满足条件，因为它的平方和立方只含有阿拉伯数字：1,3,5,6,6,8,9，像0,2,4,7就没有，而6重复了。

用传统的计算机解决这个问题，操作员将不得不采取下面的

方法。操作员将数字 1 输入进去然后让计算机进行测试。一旦计算机完成了必要的运算,它就告知这个数字是否符合标准。数字 1 不符合标准,所以操作员输入数字 2 让计算机再一次运行并测试等等。直到符合的数字最终被找到。计算机输出的答案是 69,因为 $69^2 = 4761$;$69^3 = 328509$,这些数字确实包括了那十个阿拉伯数字,而且每个只出现了一次。实际上,69 是惟一能满足这些条件的数字。可见这个过程是非常耗时的,因为传统的计算机一次只能测试一个数字。如果计算机测试一个数字要用一秒钟,那么它将花 69 秒才能找到答案。相反,一台量子计算机只需花一秒钟就能找到答案。

操作员首先要把数字表示成一种特殊的形式以利于发挥量子计算机的威力。表示数字的一种方法是利用自旋粒子的形式——许多基本的粒子都具有自旋的本性,它们要么自西向东自旋,要么自东向西自旋,就像一个篮球在指尖旋转。当一个粒子自东向西自旋时,它就代表 1,当它自西向东自旋时,就代表 0。因此,一序列的自旋粒子就代表一序列的 1 和 0,或是一个二进制数。比如说,有七个粒子,自旋方向分别是向东,向东,向西,向东,向西,向西,向西,组合起来就是 1101000 这个二进制数字,它等于十进制数 104。根据这七个粒子的自旋方向,它们的组合就能表示出 0 到 127 之间的任何数字。

用传统的计算机进行这种操作,操作员要输入一串粒子的自旋方向,就像向西,向西,向西,向西,向西,向西,向东,这代表 0000001,它仅仅表示的是十进制数 1。然后操作员就等待计算机测试这个数字,看它是否满足早先时候列出的条件。接着操作员将输入 0000010,这一序列的粒子自旋方向代表 2,依次类推。跟前面的情况一样,一次只能输入一个数字,我们知道这是很耗时的。但如果我们用量子计算机处理的话,操作员可以选择两种输入数字的方法,而且都快得多。因为使用的都是基本粒子,所以它

们遵守量子物理定律。因此,当一个粒子没有被观察时,它就处于重叠态,这就意味着它同时在两个方向都有自旋,所以它可同时代表0和1。另一种选择是,我们可以认为这个粒子进入了两个不同的宇宙:在一个宇宙它的自旋向东代表1,而在另一个宇宙它自旋向西代表0。

可以通过下面的步骤达到重叠态。假设我们能观察到其中的一个粒子,它的自旋方向是自西向东。要改变它的自旋方向,我们应该放出足够大的脉冲能量,大到使该粒子反向,自东向西地自旋。如果我们发出的是较弱一些的脉冲,那么有时我们会很幸运,粒子改变了它的自旋方向,但有时也会很不幸运;粒子仍保持其自西向东的自旋方向。到这时为止,这个粒子一直被清楚地观察着,我们能跟踪它的行踪。但如果我们把这个自西向东自旋的粒子放进一个盒子,离开我们的视野,然后向它施加一弱的脉冲能量,那么我们无法知道它的自旋方向是否改变了。粒子处在了自西向东自旋和自东向西自旋的重叠态,就像那只猫处在既死又活的重叠态。把七个自西向东自旋的粒子放进一个盒子里,然后放出七次弱的脉冲能量作业于它们,则这七个粒子都处于重叠态。

由于七个粒子都处于重叠态,它们实际上就代表了自西向东和自东向西自旋的所有可能的组合。这七个粒子同时表示了128种不同的状态或128个不同的数字。操作员将这七个粒子输入量子计算机,这七个粒子仍保持重叠态,然后计算机运行计算程序,它同时测试了全部128个数字。一秒钟后,计算机输出了满足前提条件的数字69。操作员只付出了一次代价就完成了128次计算过程。

量子计算机违背常理。先不考虑细节,量子计算机可用两种不同的方式来解释其原理,这就看你喜欢哪一种量子理论。一些物理学家的观点是量子计算机是作为一个单独的单位,同时对128各数字进行相同的运算程序。另一些物理学家则认为量子计

算机分成了 128 个单位,每一个单位各是一个独立的宇宙,一个宇宙只运行一个计算。量子计算方法是技术进步的曙光。

传统计算机是通过 0 和 1 操作的,0 和 1 叫做比特(bit),这是二进制数的简称。因为量子计算机在一量子重叠态也用 1 和 0 处理,在这儿 1 和 0 就成为量子奎比特(qubit)。当我们考虑更多的粒子时,量子比特的优势变得更明显。用 250 个自旋的粒子,或 250 个量子比特,可能代表大约 10^{75}种组合,这比宇宙中的原子数还多。如果 250 个粒子处在适当的重叠态,那么量子计算机能同时运行 10^{75}次运算程序,所有计算完成只花费一秒钟。利用量子的效力可增强量子计算机难以想像的威力,多伊奇是在 1980 年代中期提出量子计算机概念的,当时无人能想像出怎样才能造成一台坚固可用的机器。比如说,科学家不可能实际地造成某个东西来计算重叠态的自旋粒子。最大的障碍是怎样在整个计算过程中维持重叠态。重叠态只能在没被观测的情况下才会存在,从广义上讲,任何一种对重叠态的外部作用都属于观测。一个单独的偏离轨道的原子碰到某一个自旋的粒子,就会使重叠态遭到破坏,转变成一独立的状态,使量子计算失败。

另一个问题是科学家不能够设计出运行量子计算机的程序,而且不能确定这计算机适合进行哪一种类型的计算。然而在 1994 年,新泽西 AT&T 贝尔实验室的彼特·肖尔成功地勾勒出可用的量子计算机程序的雏形。引起密码学家注意的是肖尔的程序定义的一系列步骤,在量子计算机上运行能质因数分解一个很大的数——这正是解开 RSA 密码所需要的。当马丁·加德纳把 RSA 难题发表在《科学美国人》之后,600 个计算机操作员花了 17 年的时间质因数分解了一个有 129 位的阿拉伯数字。与此相反,肖尔的程序能在其几百万分之一的时间内质因数分解一个比它大一百万倍的数。但不幸的是,肖尔不能验证他的质因数分解程序,因为量子计算机还没有问世。

接着，在1996年，贝尔实验室的洛夫·格罗弗编写了又一个强大的程序。格罗弗的程序能以难以想像的高速搜寻一个列表，这听起来没有什么特别令人感兴趣的地方，直到你认识到它正是解开DES密码所需要的。要解开DES密码必须搜寻一序列所有可能的密钥，找到正确的一个。常规的计算机一秒钟内能检查一百万个密钥，那要解开DES密码需花一千年的时间，然而一台量子计算机用格罗弗的程序运行将在不超过四分钟内找到密钥。这两个量子计算机程序的出现是很巧合的，它们是密码学家最想解决的问题。尽管肖尔和格罗弗的程序让密码破解者看到了极为乐观的前景，但存在一个极大的障碍，因为仍没有一台可工作的量子计算机能运行这些程序。显然，这个在解密技术方面最终的武器所具有的潜能吊足了一些组织的胃口。比如美国国防高科技研究中心(DARPA)，洛斯阿拉莫斯国家实验室，他们拼命地想造出能处理量子比特的设备，就像处理比特的硅片。尽管最近的大量突破大长研究者的信心，但公平地讲，这项技术仍处在很低的水平。1998年，巴黎第四大学的瑟奇·哈瑞克审视了关于这些突破的说法，他否定了几年内就会诞生一台真正的量子计算机的可能。他说这就像费劲地用卡片搭好了屋子的第一层，认为然后接下来的15000层只是照搬形式而已。

只有时间能回答是否及何时建造一台量子计算机所面临的困难才能解决。在这其间，我们只能思索它将带给密码界什么样的影响。自从20世纪70年代以来，密码制造者在与密码破解者的竞赛中一直处于较领先的位置，这要感谢像DES和RSA这样密码的帮助。这些各种类型的密码是珍贵的资源，因为我们已逐渐相信它们能把我们的电子邮件加密，保护我们的隐私。同样，当我们进入21世纪，越来越多的贸易将在互联网上进行，而电子市场要依赖强大的密码保护来保证金融交易的正常进行。由于信息已成为世界上最有价值的商品，一个国家的经济、政治和军事的命运

将仰仗于强大的密码。

因此，一台完全可操作的量子计算机的发明将使我们的个人隐私处在危险的境地，电子商务遭到破坏，国家的安全受到威胁。量子计算机威胁到了世界的稳定。无论哪一个国家首先使其成为现实，都可以监控本国公民的通讯，获悉商业竞争对手的想法和偷听敌人的计划。尽管量子计算机的研究仍处在初期阶段，但它潜在威胁着个人、国际商务和全球安全。

量子密码术

当密码破解专家期待着量子计算机时代的到来时，密码专家正在为实现他们的技术奇迹而努力工作——这是一种加密系统，它将重新恢复隐私权，甚至在面对强大的量子计算机时仍能起作用。这个新式的加密术基本上和我们以前提到的都不一样，它给了我们拥有完美隐私权的希望。换句话说，这个系统是没有缺陷的，它将永远保护我们绝对的安全。而且，它是以量子理论为基础的，和量子计算机使用的是一样的理论基础。所以当量子理论给计算机提供了启发，使之能破解现在存在的所有的密码，它同时也是不可破解的新式密码——量子密码系统的核心。

关于量子密码系统的故事要追溯到20世纪60年代末，哥伦比亚大学的毕业生斯蒂芬·威斯纳的一个奇特的想法。遗憾的是，威斯纳不幸过早创立了这个想法，得不到任何人的重视。他仍能回想起他的长辈的反应："我没有从我的论文指导老师那里得到任何支持——他对这个根本不感兴趣。我拿给其他人看，他们都露出很奇怪的表情，然后就去干他们正在做的事。"威斯纳提出的是奇特的量子货币概念，在防止造假币方面有很大的突破。

威斯纳的量子货币很大程度上依赖光子物理学。当一个光子

在空间运动时,光子是振动的,如图 73(a)所示。所有四个光子沿着同一方向运动,但每一个的振动角度不同。振动的角度就是所知的光子的偏振现象,一个光球发出所有振动方向的光子,意思是说一些光子上下振动,一些左右振动,其他的振动角度在二者之间。把问题简单化,我们假设光子只有四种偏振,我们将其表示为↕,↔,↘和↗。

在光子的运动路径上放一个滤光器——偏振片,它只允许一束光中某一特定振动方向的光子通过;换句话说,透过的光子具有相同的偏振。在一定程度上,我们可以把偏振滤光片看作是一个栅栏,把光子看作是随意分散在栅栏上的火柴梗。只有火柴梗具有正确的角度才可能滤过栅栏。任意一个光子只要具有与偏振滤光片相同的偏振方向就能自动穿过偏振片而不发生变化,与偏振片的偏振方向垂直的光子就会被阻挡。

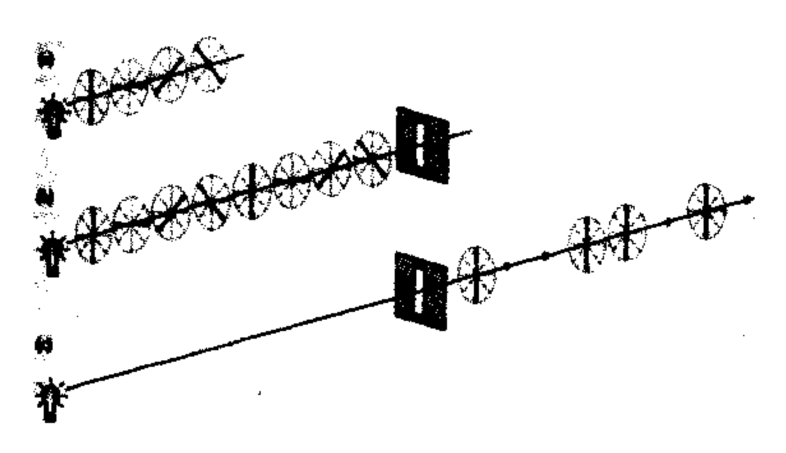


图 73:光子穿越光栅的示意图

不幸的是,当我们考虑对角方向偏振的光子接近偏振方向垂直的偏振片时,用火柴梗类比就行不通。虽然对角方向的火柴梗

不能漏过方向垂直的栅栏，但这对于对角方向偏振的光子接近偏振方向垂直的偏振滤光片是没有什么困难的。实际上，当对角方向偏振的光子面对偏振方向垂直的偏振滤光片时，其处于量子困境(quantum quandary)。接下来发生的事情是，其中随机的一半被阻挡，另一半穿过偏振片，那些穿过去的光子将变成垂直方向偏振。图 73(b)显示的是八个光子接近一个偏振方向垂直的偏振滤光片，图 73(c)显示只有四个光子成功地穿了过去。所有垂直方向偏振的光子都穿过了偏振片，所有水平方向偏振的光子都被阻挡了，对角方向偏振的光子有一半穿过了偏振片。

这种能阻挡某几种光子的性质可用于制造偏振光太阳眼镜。事实上，你可以用一副偏振光太阳眼镜来验证偏振滤光片的作用。首先拿下一片透镜，然后闭上这边的眼睛，用另一只眼睛通过剩下的那片镜片看。不足为怪的是，世界看起来很黑，因为透镜挡住了许多光子，否则这些光子会到达你的眼睛。在这个时候到达你的眼睛的都是相同偏振方向的光子。接下来，把拿下来的那片镜片放在你戴的那片镜片前面，并且慢慢地转动它。旋转到一个点时，活动的镜片对到达你的眼睛的光量没有任何影响，因为它的方向和固定的镜片是一样的——所有能透过活动的镜片的光子也就能透过固定的镜片。如果这时你将活动的镜片旋转 90°，你的视野完全变黑了。在这个组合时，活动的镜片的偏振方向和固定镜片的偏振方向是垂直的，透过了活动镜片的光子就会被固定镜片阻挡下来。如果现在你把活动镜片再旋转 45°，那么就到达两透镜部分不重合的中间阶段，透过活动镜片的光子中有一半设法透过了固定镜片。

威斯纳计划利用光子的偏振性质来制造纸币，这种方法可以防止被伪造。他的想法是在钞票上设置 20 个陷光器，这种微型装置可以捕捉并保留住一个光子。他建议银行用四片偏振滤光片，各是不同的偏振方向(↕，↔，↘，↗)，再用一定顺序的 20 个偏振

光子填满那 20 个陷光器，每一张纸币上的顺序都不同。举个例子，如图 74 所示一张纸币上的偏振方向顺序为(⤡，↕，⤢，⤢，↔ ↕，↕，⤡，↕，⤡，↔，↔，⤢，↔，⤡，⤢，↔，⤢，↕，↕)。尽管偏振方向在图 74 中明确的显示出来，但实际上它用肉眼是看不出来的。每一张纸币还会带有一个传统的有顺序的数字，图中所示的美元钞票的序号是 B2801695E。发行银行可以在每一张钞票上同时用偏振序列和印刷序列号作标记，然后保留一张原版的表，记录序列号和相对的偏振序列。

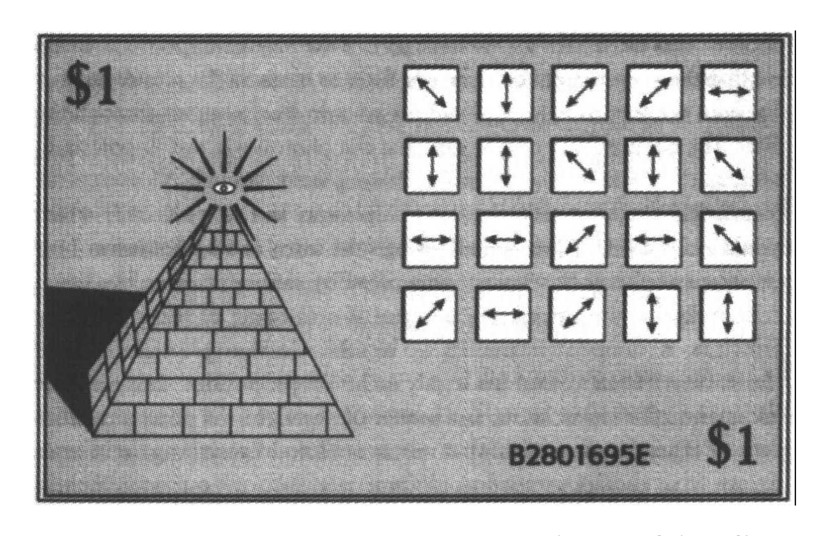


图 74：威斯纳的光子钱币，每一张都有不同的清晰可见的序号，并且 20 个陷光器的面积是保密的。陷光器包含着不同偏振方向的光子。银行根据不同的序号就知道每张纸币上的光子偏振方向是什么，但造假币者却不知道。

造假币者现在要面对一个很大的问题——他不能仅仅是用一个任意的序列号和任意一种陷光器中的偏振序列来伪造一张美

钞,因为这种配对不会出现在银行的原版记录表上,银行会发现这张钞票是假币。要造出一张难以鉴别的假币,造假币者必须以一张真币作样版,用某种方法测出它的 20 个偏振方向,然后就可以造出一张复制的美钞,再复制序列号,以正确的顺序安排陷光器。然而,测光子的偏振方向是一件众所周知的很困难的工作,如果造假币者不能准确地测出真币的偏振方向序列,那么他别指望能造出一张复制美钞。为了理解测量光子的偏振方向的困难,我们需要考虑好我们应该怎样着手试着完成这样的测试方法。要弄清楚光子的偏振方向只有惟一的方法,就是用偏振滤光片。要测出一个特定的陷光器中的光子的偏振方向,造假币者得选一个偏振滤光片并放在一个特定的方向上,比方说垂直方向↕。如果从这个陷光器中脱离的光子碰巧就是垂直方向偏振,它就会透过这个偏振方向垂直的偏振滤光片,那么造假币者就能准确地认为它是垂直方向偏振的光子。如果这个脱离的光子是水平方向偏振,它就不可能透过偏振方向垂直的偏振滤光片,造假币者就能确定这是水平方向偏振的光子。但是,如果这个脱离的光子碰巧是对角方向偏振⤡或⤢,它可能透过或不透过滤光片,这两种情况都会使造假币者无法确定该光子的种类。一个⤡方向偏振的光子可能透过偏振方向垂直的偏振滤光片,这种情况下造假币者会错误地认为这是一个偏振方向垂直的光子,或者是相同类型的光子没有透过滤光片,这个结果会让他错误地判断这个光子的偏振方向是水平的。另一种选择是,造假币者用偏振滤光片测另一个陷光器中的光子,把滤光片放在比如⤡方向上,这样能准确地鉴定出偏振方向为对角的光子,但就不可能正确地测出偏振方向垂直或水平的光子。造假币者的问题是他必须用偏振方向正确的偏振滤光片来鉴定一个光子的偏振方向,但他不知道用哪一个方向,因为他不知道光子的偏振方向。这"第二十二条军规"是光子固有的物理性质的一部分。假设造假币者选用⤡方向滤光片来测从第二个陷光器中

脱离的光子，这个光子没有透过滤光片。造假币者能肯定的是这个光子不是↘方向偏振，因为这个方向偏振的光子才会透过滤光片。然而，造假币者不能断定这个光子的偏振方向是↙，这个方向当然是不可能透过滤光片的，或者它的偏振方向是↔抑或↕，它们各有50%的机会被阻挡。

测量光子的难度是测不准原理的一个方面，这个原理是德国物理学家海森伯格提出的。他把高度专业的理论用通俗易懂的话表述出来："原则上说，我们不可能知道现在所有的细节。"这并不意味着我们不能够知道每一件事，只是因为我们没有足够的测量设备，或者是因为我们的设备设计太差。相反，海森伯格声称逻辑上是不可能以绝对的精确度测量一特定物体的每一个方面的。在这个特定的事件中，我们不可能以绝对的精确度测出在陷光器中的光子的每一个方面。测不准原理是量子理论的又一个令人惊异的结论。

威斯纳的量子货币依赖于制造假币是分两阶段进行的操作这个事实：首先造假币者需要非常精确地测量真币，然后才能复制。威斯纳在美元的设计中加入了光子，使得这种钞票不可能测准，因此，这就给制造假币设置了障碍。

一个天真的造假币者会想如果他不能测出陷光器中光子的偏振方向，那么银行也不能。他就可以用任意的偏振方向序列填满陷光器来制造假美元。但是，银行是能证明那一张钞票是真的。银行会根据序列号去核对那张机密的原版记录表，看哪一个光子应该在哪一个陷光器中。因为银行知道每一个陷光器中光子的偏振方向，所以可以正确地决定放置偏振滤光片的方向准确地测量每一个陷光器中的光子。如果钞票是伪造的，造假币者设置的随意的偏振方向序列就会导致错误的测量结果，然后这张钞票就被视为假币。举个例子，如果银行用↕偏振方向的滤光片应该测出↕偏振方向的光子，但发现光子被滤光片阻挡了，那么就可以知道

造假币者在这个陷光器中填入了错误的光子。不过,如果这张钞票是真的,那么银行将用适当的光子重新填满陷光器,再发放回流通领域中。

简而言之,造假币者不能测出真币中的偏振方向序列,因为他不知道每一个陷光器中的光子是哪一种类型,因此也就不可能知道怎样才能正确设置偏振滤光片的方向进行测量。另一方面,银行就能检查真币的偏振方向序列,因为最初的序列是它设置的,所以银行知道在每一个陷光器应该用哪种偏振方向的滤光片。

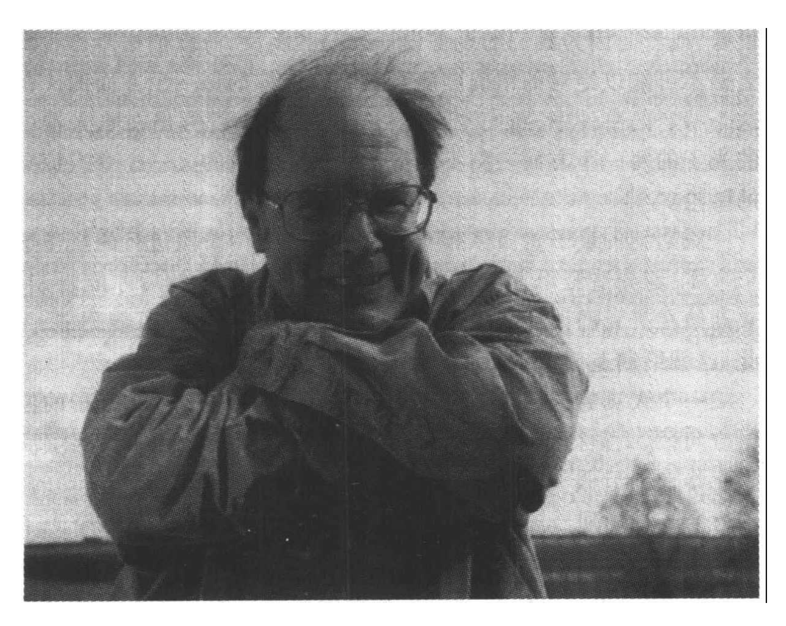


图 75:查尔斯·贝内特

量子货币是一个十分聪明的想法。但也是不能实行的。首先,工程师们还没有开发出一种技术能捕捉一种特定偏振方向的

光子并保持很长时间。甚至即使是这种技术存在,也会因为价格昂贵而无法实施。可能要花费大约一百万美元来保护每一张美钞。尽管不可能实施,但量子货币这个想法是以一种迷人和富有想像力的方式应用了量子理论。所以,即使得不到论文指导老师的鼓励,威斯纳还是向一家科学期刊投了稿,但被退稿了。他投稿到其他三家期刊,又被退稿三次。威斯纳认为他们只不过是没有理解物理罢了。

似乎只有一个人能分享威斯纳提出量子货币概念后的兴奋。他是威斯纳的一位老朋友查尔斯·贝内特,早些年前,他和威斯纳是布兰德斯大学的同学。贝内特对科学的每一个方面都充满了好奇心,这是他个性中最突出的特点。他说他知道三岁时他的理想是成为科学家,他在童年时对科学的爱好得到了他母亲的鼓励。有一天她母亲回到家发现灶上有一个平底锅,里面炖的肉汤已经沸腾了。幸好她没有想过要尝一尝,因为这其实是一只海龟的残留物,这是小贝内特干的,他要用碱煮掉骨头上的肉,这样就能得到一副完整的海龟骨架标本。贝内特十几岁时,他的兴趣从生物转向了生物化学,当他到布兰德斯上学时,他就决定主攻化学。从学校毕业后他又迷上了物理化学,后来他在物理、数学和逻辑方面都做过研究工作,现在他从事计算机科学的研究。

威斯纳知道贝内特兴趣广泛,他希望贝内特会欣赏量子货币,就把他被退稿的论文副本拿给贝内特看。贝内特马上就对这个概念着了迷,并觉得这是他见过的最漂亮的想法。在以后的十多年,他会偶尔把那篇文章再读一次,想着是否有一种方法能将如此具有独创性的想法变成有用的东西。甚至在贝内特成为IBM托马斯·J·沃森实验室的研究员时,他仍在思考威斯纳的想法。期刊不想刊登这篇文章,但贝内特却迷上了它。

一天,贝内特把量子货币的概念解释给蒙特利尔大学的计算机科学家吉勒斯·布拉萨德听。贝内特和布拉萨德在不同的研究

项目上都有合作,他们一遍又一遍地讨论威斯纳论文中复杂的问题。渐渐的,他们发觉威斯纳的想法可能可以运用于密码学。伊芙要译解艾丽丝和鲍勃的加密通信,首先她必须以某种方式正确截取到传输出来的内容。威斯纳的量子货币之所以是安全的,是因为不可能正确地获悉美元里捕捉的光子的偏振方向。贝内特和布拉萨德想知道如果加密的信息用一序列偏振的光子表示和传送的话会发生什么样的情况。理论上,伊芙似乎是不能准确地读到这样加密的信息的,如果她不能读到这些加密信息,那她就不能译解这个信息。

贝内特和布拉萨德开始根据下面的原理编一个系统。假设艾丽丝想发给鲍勃一条加密的信息,由一序列的 1 和 0 组成。她用激发的特定偏振方向的光子表示 1 和 0。艾丽丝有两种方案使 1 和 0 与光子的偏振方向联系起来。第一种方案称为“直线式”或“+ - 方案”,她激发↕ 光子代表 1,↔光子代表 0。另一种方案称为“对角式”或“× - 方案”,她激发↗ 光子代表 1,↖ 代表 0。要发出一个二进制的信息,她可以任意使用这两种方案。因此,这个二进制的信息可以下面的形式传出:

信息:1　1　0　1　1　0　1　0　0　1

方案:+　×　+　×　×　×　+　+　×　×

传输:↕　↗　↔　↗　↗　↖　↕　↔　↖　↗

艾丽丝发出第一个 1 用了“+ - 方案”,第二个 1 用了“× - 方案”。因此,1 是用两种方式传出的,但每一次只能用一个偏振光子表示。

如果伊芙想截取这个信息,那她需要确定每个光子的偏振方向,就像造假币者要确定美钞里面的陷光器中的每一个光子的偏振方向。伊芙要想测出每一个光子的偏振方向,她必须决定好在每一个步骤时怎样确定偏振滤光片放置的方向。她不可能确切地知道艾丽丝对每个光子使用了哪一种方案,所以她选择偏振滤光

片时只能是偶然的并且有50%的错误概率。因此她不可能得到传输出来的全部内容。

用一个简单一些的方法考虑伊芙进退两难的困境，就是假装在这种形式下，伊芙有两种类型的偏振检测器。“+型检测器”能非常准确地测出水平和垂直偏振的光子，但不能确定地测出对角方向偏振的光子，仅仅是把它们误认为水平或垂直方向偏振的光子。另一种情况，“×型检测器”则能非常准确地测出对角方向偏振的光子，但不能确定地测出水平和垂直偏振的光子，把它们误认为是对角方向偏振的光子。比如说，如果她用“×型检测器”测量第一个光子它是↕，她会误认为它是⤢或⤡。如果她把它错认为⤢，那她还不会有麻烦，因为这也代表1，但如果她错认为⤡，那么她就有很大麻烦了，因为这个代表0。对伊芙来说更糟的是，她只有一次机会准确地测量光子。一个光子是不可分割的，所以她不能把它分成两个光子，用两种类型的检测器测它。

这个系统似乎有一些令人高兴的特点。伊芙不能确定准确地截取加密的信息，所以她没有破译的希望。然而，这个系统遇到了一个严重的而且显然不可能克服的问题——鲍勃将碰到和伊芙一样的困境，因为他也无法知道艾丽丝对每一个光子的偏振方向是用什么方案决定的，所以他也会把信息读错。解决这个问题很明显的一个方法是，艾丽思和鲍勃在每一个光子上会用哪一种偏振方案达成一致。就上面的例子来说，艾丽丝和鲍勃会共享一张表或是密钥，可以读出+×+×××++××。但我们又回到了密钥分配的老问题上——艾丽丝必须以某种方式把偏振方案表安全地送给鲍勃。

当然，艾丽丝可以使用像RSA这样的公开密钥密码给这张方案表加密，然后把它发给鲍勃。但想像一下，我们现在生活在RSA被破解的时代，也许还伴随着强大的量子计算机的发展。贝内特和布拉萨德的系统必须独立使用而不依赖RSA。几个月的

时间里，贝内特和布拉萨德试图想出解决公开密钥分发问题的方法。1984 年，两人在离 IBM 托马斯·J·沃尔森实验室不远的科洛顿——哈蒙火车站的月台等火车。布拉萨德要乘火车返回蒙特利尔，为了熬时间就闲聊起艾丽丝、鲍勃还有伊芙所作的尝试和面临的困难。如果火车早到几分钟，他们可能已经道别了，而密钥分发问题就不会有进展。是的，他们想出来了！就是这一段时间，他们创立量子密码术，这是发明出来的最安全的密码术。

运用量子密码术需要三个预先发生的过程。虽然这些事件不包括发出加密的信息，但他们确实使密钥安全地交换了，这个密钥要用于加密信息。

过程 1，艾丽丝为起始，任意发送了一序列的 1 和 0(比特)，任意选择直线式(水平和垂直方向偏振)和对角式偏振方案。图 76 显示的是这样的一序列光子在传送给鲍勃的途中。

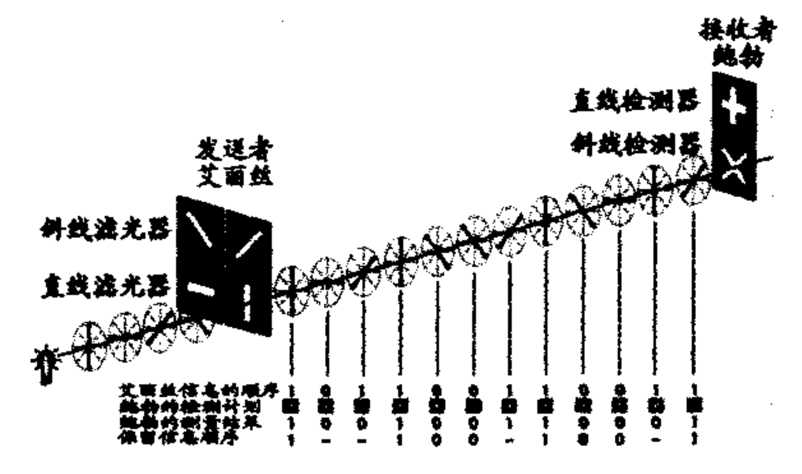


图 76：该图显示的是一个序列光子在传送给鲍勃的途中

过程 2，鲍勃要测出这些光子的偏振方向。由于他不知道艾丽丝对每个光子使用的是哪一种偏振方案，他只能交换尝试“+型

检测器”和“×型检测器”。有时鲍勃挑选的是正确的检测器，有时他的选择又是错误的。如果鲍勃用错了检测器，那他也会错判艾丽丝发出的光子的偏振方向。表 27 列举了所有的可能性。

比如说，在上面的一行里，艾丽丝用直线式方案发出 1，那么传送的是↕光子；那么鲍勃用了正确的检测器，所以他检测出是↕光子，然后正确地记录下这个序列的第一个比特是 1。在下一行里，艾丽丝采用了相同的方案，但鲍勃用错了检测器，所以他可能检测出↗光子或↖光子，这就意味着他可能正确地记录下 1 或者错误地记成 0。

过程 3，这个时候，艾丽丝已经发出了一个序列的 1 和 0，鲍勃也正确和不正确地检测了一部分。为了使状况明了，艾丽丝通过普通的不安全的电话线打电话给鲍勃，告诉鲍勃她对每一个光子用的是哪一种偏振方案——但不告诉每一个光子具体的偏振方向。所以她可能说的是第一个光子用的是直线式方案，但她不会说出她发出的是↕光子还是↔光子。然后鲍勃告诉艾丽丝他猜对了哪一个比特的偏振方案。他肯定测对了这些比特偏振方向的，而且正确地标记出是代表 1 还是 0。最后艾丽丝和鲍勃舍去了鲍勃用错误的方案测量的光子，把他用对了方案测出的集中起来。结果他们得到了一个新的短一些的比特序列，由鲍勃测出的正确结果组成。整个过程如图 76 所示。

经过这三个过程，艾丽丝和鲍勃得到一系列普通的阿拉伯数字，就像图 76 中得到的序列 11001001。这个序列最重要的性质是它是随机的，因为它来源于最初从艾丽丝发出的序列，那个序列也是随机的。此外，鲍勃使用正确的检测器的时机也是随机的。这个经过协商同意的序列并不含有信息，但它能成为一个随机产生的密钥。最后，真正安全的加密步骤可以开始了。

这个达成一致的随机产生的序列可以被用作一个“一次性便签”密码的密钥。在第三章里就已经讲过一个随机的字母或数字

序列，也就是“一次性便签”，使你产生一个不可破解的密码——这不只是操作上不可能，而且是绝对的不可能。以前，“一次性便签”密码惟一的问题是安全分发随机序列的困难，但贝内特和布拉萨德的计划克服了这个困难。艾丽丝和鲍勃已经得到了一致的“一次性便签”密钥，并且量子物理定律使伊芙根本不可能成功地截获密钥。现在我们从伊芙的角度出发，那我们就可以看看为什么她不可能截获这个密钥。

表 27：在过程 2 中艾丽丝与鲍勃交换光子的所有可能性方案

艾丽丝的计划	艾丽丝的信息	艾丽丝发送的光子	鲍勃的检波器	正确的检波器	鲍勃检测的光子	鲍勃的信息	鲍勃的信息是正确的吗？
直线	1	↕	+	Yes	↕	1	Yes
			×	No	⤢	1	Yes
					⤡	0	No
	0	↔	+	Yes	↔	0	Yes
			×	No	⤢	1	No
					⤡	0	Yes
斜线	1	⤢	+	No	↕	1	Yes
					↔	0	No
			×	Yes	⤢	1	Yes
	0	⤡	+	No	↕	1	No
					↔	0	Yes
			×	Yes	⤡	0	Yes

当艾丽丝传出偏振光子时,伊芙试图测量它,但她不知道该用“+型检测器”还是“×型检测器”。有一半的几率她会选错检测器。这和鲍勃遇到的情况完全相同,因为他也是50%的选错概率。但是,在传送后,艾丽丝告诉鲍勃对每一个光子他应该用哪一种方案,而且他们同意只用鲍勃用正确的检测器测出的光子。但这对伊芙一点帮助也没有,因为可能有一半的光子是她用错误的检测器测出的,所以也就不会截取到组成最终密钥的那一部分光子。

用一副扑克牌来讲量子密码术要比以偏振光子讲好理解。每一张牌都有花色和数字,就像红心J、梅花6,通常我们都是同时看一张牌的花色和数字。假设只可能要么看花色,要么看数字,二者不能同时知道。艾丽丝从一副牌里抽了一张,并决定是看花色还是看数字。假设她选择看花色,结果是“黑桃”,她记了下来。这张牌恰好是黑桃4,但艾丽丝只知道是一张黑桃。然后她通过电话线传给了鲍勃。这时候发生的是,伊芙也要看这张牌,但不幸的是她选择看的是牌的数字,结果是“4”。当鲍勃收到这张牌时,他决定看牌的花色,结果仍然是“黑桃”,他也记录了下来。之后,艾丽丝打电话给鲍勃,问他是否看的是花色,他说是的,因此艾丽丝和鲍勃他们共享了某个共有的信息——他们都把“黑桃”记在了笔记本上。然而,伊芙笔记本上记的是数字“4”,这根本一点用也没有。

接着,艾丽丝从这副牌里又抽出一张牌,是方块K,但她又只能看一种性质。这次她选择看牌的数字,结果是“K”,然后同样用电话线传送给鲍勃。伊芙也要看这张牌,而且她也选择了看数字,得到结果“K”。当鲍勃接到牌时,他决定看的是花色,结果是“方块”。

之后,艾丽丝打电话给鲍勃问她看的是不是数字,他不得不承认他猜错了,他看的是花色。艾丽丝和鲍勃不会为此烦恼,因为他们可以把这张特殊的牌完全舍去,再从那副牌中抽一张再来一次。

这一次伊芙猜对了，她和艾丽丝看的都是“K”，可是这张牌作废了，因为鲍勃看错了。所以鲍勃不必为他的错误担心，因为艾丽丝和他已经协商好舍去这张牌，而伊芙只能坚持她的错误结果。事发出几张牌后艾丽丝和鲍勃共同协商得到了一个序列的花色和数字组合，然后就可以用作某种密钥的主要组成成分。

量子密码术使艾丽丝和鲍勃共同协商确定了一个密钥，而伊芙却不可能不犯错地截取到这个密钥。此外，量子密码术还有一个额外的好处：艾丽丝和鲍勃利用这个方法可以发现伊芙是否在窃听。伊芙在电话线上窃听会很暴露，因为她每测一次光子就会冒改动光子偏振方向的风险，这些改动对于艾丽丝和鲍勃来说太明显了。

假设艾丽丝发出的是⤡光子，而伊芙用错误的检测器“+型检测器”进行了测量。会发生这样的结果，“+型检测器”会迫使射入的⤡光子透过滤光片后变成↕光子或↔光子，因为这是这种光子透过了伊芙所使用的检测器后只会出现这种情况。如果鲍勃测量这个改变了的光子时，用了“×型检测器”，那么他可能测得的是⤡光子，也就是艾丽丝发出的那个类型，而他也可能测到的是⤢光子，这就造成了误读。对艾丽丝和鲍勃来说这就出现了一个问题，因为艾丽丝发出的是对角方向偏振的光子，并且鲍勃用的是正确的检测器，然而他测到的结果却是错误的。简单地说，当伊芙用错的检测器测量光子时，她会使其中的某些光子的偏振方向发生转动，这就使鲍勃可能测错，甚至是他用了正确的检测器时他也会错。当艾丽丝和鲍勃进行短暂的错误检查程序时就能发现这些错误。

错误检查是在前面提到的三个预备过程发生后进行的，到这个时候，艾丽丝和鲍勃应该已经得到了同样的1和0序列。假设他们确定了长1075位的二进制数序列。艾丽丝和鲍勃检查他们各自的序列是否相符的方法是艾丽丝打电话给鲍勃，并把她的完

整序列告诉鲍勃。不幸的是，如果伊芙正好在窃听，她就能截取到完整的密钥。检查全部的序列显然是不明智的，也是没有必要的。相反，艾丽丝只需随机地检查75个数就可以了。如果鲍勃同意检查这75个数，那么对伊芙来说，几乎不可能在原来的光子传输的过程中进行窃听。实际上，伊芙通过电话线截取光子时而不影响到鲍勃测量这75个数的机会是百万分之一。由于这75个数是艾丽丝和鲍勃公开讨论过的，所以，这些数要被舍去，他们的"一次性便签"就从1075位二进制数减为1000位，这样一来，如果艾丽丝和鲍勃发现在这75个数中有前面提到的矛盾的地方，那么他们可以判断伊芙在窃听，他们就会放弃整个"一次性便签"，换一条新的线路，全部从头开始。

总的说来，量子密码术这个系统确保了信息传递的安全，使伊芙很难正确地截取到艾丽思和鲍勃间的通信。还有，如果伊芙试图窃听的话，艾丽丝和鲍勃也能查出她的存在。因此，量子密码术使艾丽丝和鲍勃可以完全秘密地交换和协商"一次性便签"，之后他们就能把这个"便签"当作密钥来加密信息。这个过程有五个基本的步骤：

(1)艾丽丝发给鲍勃一个光子序列，然后鲍勃测量光子的偏振方向。

(2)艾丽丝告诉鲍勃他测的结果中哪一些使用的是正确的检测器。（虽然艾丽丝告诉鲍勃他用对了哪几次检测器，但她不会告诉鲍勃正确的结果应该是什么，所以这种通话会被监听，但不会影响安全性。）

(3)艾丽丝和鲍勃舍去鲍勃不正确的测量结果，把他测对的结果集中起来，组成一对同样的"一次性便签"。

(4)艾丽丝和鲍勃检查整个"一次性便签"中的几个数。

(5)如果查对过程令人满意，他们就能用这个"一次性便签"加

密信息;如果这次查对出现错误,他们可以断定伊芙截取了光子进行测量,他们需要重新开始。

在威斯纳关于量子货币的论文被科学期刊退稿 14 年后,这篇文章促成了一个绝对安全的通讯系统的产生。现居住在以色列的威斯纳终于从这个曾经困扰他的事件中解脱了,他的工作得到了承认,他说:“回到从前,我怀疑是否我没有付出更多。大家觉得我是懦夫,没有尽更大的努力发表我的文章——我想在一定程度上来说他们是对的,但那时我只是一个刚毕业的学生,我没有那么多的信心。所以无论如何是不会有人对量子货币感兴趣的。”密码学家们热烈地祝贺贝内特和布拉萨德创立了量子密码术。然而,许多经验主义者争论这个系统在理论上行得通,但在实际操作时就会失败。他们相信处理单个光子是很困难的,这将使这个系统无法实现。不管批评方的意见如何,贝内特和布拉萨德确信量子密码术可以实际实施。事实上也是,他们坚信他们的系统都不需要仪器来验证。正如贝内特曾经把这作了比喻:“如果你知道北极点在哪,你何必要亲自去那儿才确认。”

但持怀疑态度的人越来越多,终于激起贝内特去证明这个系统确实能实际操作。1988 年,贝内特开始为量子密码系统准备所需要的条件,他还让一个研究生约翰·斯莫林帮忙集中所需设备。经过一年时间的努力,他们准备好了试发第一条用量子密码保护的信息。一个深夜,他们回到他们的避光实验室,这个完全黑暗的环境可以排除离散光子对试验的干扰。吃过一顿丰盛的晚餐后,他们都准备好熬夜,摆弄这些仪器。他们开始试着发出偏振光子穿过房间,然后用“+型检测器”或“×型检测器”测量光子的偏振方向。一台起名为艾丽丝的计算机将最终控制光子的传送,另一台名叫鲍勃的计算机决定用哪一种检测器测量光子的偏振方向。

调整仪器几个小时后,大约在凌晨三点,贝内特见证了第一个

量子密码的交换。艾丽丝和鲍勃设法发出和接收到了光子,它们也讨论过了艾丽丝用的偏振方案,并舍去了鲍勃用错的检测器测得的结果,协商得到了由剩下的光子组成的"一次性便签"。贝内特回忆说:"根本不用怀疑这个系统能不能工作。""只可能是我们的手指太笨了建不出来罢了。"贝内特的试验证明两台计算机(艾丽丝和鲍勃)可以绝对安全地通讯。这是历史上一个很著名的试验,尽管这两台计算机只相隔 30 厘米远。

自贝内特的试验到现在,挑战就变成建造一个可以在实用的长距离中操作的量子密码系统。这不是一个微不足道的工作,因为光子在长距离传输过程中会出问题。如果艾丽丝通过空气传输一个特定偏振方向的光子,空气中的分子会和这个光子发生作用,引起其偏振方向的改变,这是无法接受的。更有效地传输光子的媒介是通过光纤,研究者最近成功地用这项技术建立了可长距离操作的量子密码系统。1995 年,研究者在日内瓦大学成功地实现了,在长达 23 公里的光纤上把量子密码从日内瓦传到了尼翁。

最近,一群洛斯阿拉莫斯国家实验室的科学家在新墨西哥又开始在空气中试验量子密码术。他们最终的目的是建立卫星传送的量子密码系统。如果这能实现的话,就能绝对地确保全球通讯的安全。迄今为止,洛斯阿拉莫斯的研究小组成功地在空气中将量子密钥传出了 1 公里远。

安全专家现在想知道量子密码术成为一项实用的技术还需要多长的时间。这段时间量子密码术研究没有再取得进展,因为 RSA 密码已经给我们提供了实际操作上不可破解的加密方法。但如果量子计算机真的实现了,那么 RSA 还有所有其他现代密码就没有用了,量子密码术才会成为必需品。所以竞赛还在继续。真正重要的问题是量子密码术是否会及时出现,把我们从量子计算机的威胁中解救出来,或是在量子计算机发展和量子密码术出现之间的一段时期是否会造成隐私权空白。迄今为止,量子密码

术算是较先进的科技。瑞士人的光纤试验证明,在一个城市的金融机构间建立一个可以安全通讯的系统是可行的。当然,现在就可能在白宫和五角大楼之间建立量子密码联系。也许,这种联系已经存在了。

量子密码术将标志着密码制造者和密码破解者之间的战争的结束,密码制造者是最后的胜利者。量子密码术是不可破解的加密系统。这个断言确实有点夸大,特别是前面的章节中也有过类似的断言。前两千年中的不同时期,密码学家相信过单码代替密码,多码代替密码,还有机器密码如恩格玛码都是不可破解的。每一段历史中,最终都证明密码学家错了,这是因为在历史上的某个时期,他们的断言都只是基于密码的复杂程度超出了译解密码者的才智和技术这一事实。事后,我们能看到译解密码者都不可避免地找出了破解每个密码的方法,或是改进了技术来破解密码。

然而,断言量子密码术是安全的,本质上不同于以前所有的断言。量子密码术不仅在实际操作上不可破解,其他方面也是绝对不可破解的。量子理论是物理学史上最成功的理论,这就使得伊芙不可能正确地截取到艾丽丝和鲍勃建立的"一次性便签"密钥。伊芙甚至不可能不让艾丽丝和鲍勃知道她在试图截取这个"一次性便签"密钥。确实是,如果一条用量子密码保护的信息被破译了,这将意味着量子理论是有缺陷的,而物理学家就要推翻他们的结论;被迫重新思考他们对宇宙在最基本的层次运作原理的理解。

如果量子密码系统能实现长距离操作,则密码的发展将会停止。隐私权的追求也就走到了尽头。这项技术将用来保证政府、军队、商业还有公众通讯的安全。剩下的问题就是政府是否允许我们使用这些技术。还有政府怎样规范量子密码,使它只对信息时代有益,而不是保护犯罪?

附录 向密码挑战

得到 15000 美元的 10 个关口

向密码挑战开始于 1999 年 9 月，自本书英文版付印以来无人能解。这是一个测试你的解密技术和获得 15000 美元奖金的绝好机会。此次挑战共分 10 关。第一关是相对直观的单码代替密码，其他的步骤则是按照书中所述密码学的历史进程排序的。也就是说，第二关所使用的是一种最早期的密文形式，而第 10 关则是最现代的密文形式。总之，每一关都会比前一关难一些。

为了赢得奖金你需要做什么？

解开 10 个密文中的任何一篇都会得到一条信息。除了每条信息的正文以外，你会得到一个清晰明了的密码单词。如想赢得奖金，你必须集全所有 10 个密码单词，所以你必须解开 10 个密文。当然你也可以不按顺序的解开密文，但我建议你最好还是按

给出的顺序解,因为有时过一个关会为下一个关提供一些信息。

你怎样赢得奖金?

如想赢得奖金,请把你解开的每个密码单词中头两个字母寄给我们,并写明你的名字、地址和电话号码。如果你所寄的字母是正确的,我们将会在接到你的字母 28 天内与你联系,并会让你寄来 10 个完整的密码单词。如果你是第一个正确地破译所有 10 个密码单词的人,你将会赢得 15000 美元。所有信息必须寄往指定地点:

The Cipher Challenge, P.O.Box 23064, London W113 GX, UK.

获奖者将是第一个破译的人。除了依靠智力之外没有任何侥幸的成分。请注意,我只与得到正确字母的竞争者联系。除此之外,我不会回答任何关于密码挑战的问题。任何最新的信息将被登在密码挑战的专有网址:

http://www.4thestate.co.uk/cipherchallenge.

第一关：简单的单字母替换密码

BT JPX RMLX PCUV AMLX ICVJP IBTWXVR CI M LMT'R PMTN, MTN YVCJX CDXV MWMBTRJ JPX AMTNGXRJBAH UQCT JPX QGMRJXV CI JPX YMGG CI JPX HBTW'R QMGMAX; MTN JPX HBTW RMY JPX QMVJ CI JPX PMTN JPMJ YVCJX. JPXT JPX HBTW'R ACUTJXTMTAX YMR APMTWXN, MTN PBR JPCUWPJR JVCUFGXN PBL, RC JPMJ JPX SCBTJR CI PBR GCBTR YXVX GCCRXN, MTN PBR HTXXR RLCJX CTX MWMBTRJ MTCJPXV. JPX HBTW AVBXN MGCUN JC FVBTW BT JPX MRJVCGCWXVR, JPX APMGNXMTR, MTN JPX RCCJPRMEXVR. MTN JPX HBTW RQMHX, MTN RMBN JC JPX YBRX LXT CI FMFEGCT, YPCRCXDXV RPMGG VXMN JPBR YVBJBTW, MTN RPCY LX JPX BTJXVQVXJMJBCT JPXVXCI, RPMGG FX AGCJPXN YBJP RAMVGXJ, MTN PMDX M APMBT CI WCGN MPCUJ PBR TXAH, MTN RPMGG FX JPX JPBVN VUGXV BT JPX HBTWNCL. JPXT AMLX BT MGG JPX HBTW'R YBRX LXT; FUJ JPXE ACUGN TCJ VXMN JPX YVBJBTW, TCV LMHX HTCYT JC JPX HBTW JPX BTJXVQVXJMJBCT JPXVXCI. JPXT YMR HBTW FXGRPMOOMV WVXMJGE JVCUFGXN, MTN PBR ACUTJXTMTAX YMR APMTWXN BT PBL, MTN PBR GCVNR YXVX MRJCTBRPXN. TCY JPX KUXXT, FE VXMRCT CI JPX YCVNR CI JPX HBTW MTN PBR GCVNR, AMLX BTJC JPX FMTKUXJ PCURX; MTN JPX KUXXT RQMHX MTN RMBN, C HBTW, GBDX ICVXDXV; GXJ TCJ JPE JPCUWPJR JVCUFGX JPXX, TCV GXJ JPE ACUTJXTMTAX FX APMTWXN; JPXVX BR M LMT BT JPE HBTWNCL, BT YPCL BR JPX RQBVBJ CI JPX PCGE WCNR; MTN BT JPX NMER CI JPE IMJPXV GBWPJ MTN UTNXVRJMTNBTW MTN YBRNCL, GBHX JPX YBRNCL CI JPX WCNR, YMR ICUTN BT PBL; YPCL JPX HBTW TXFUAPMNTXOOMV JPE IMJPXV, JPX HBTW, B RME, JPE IMJPXV, LMNX LMRJXV CI JPX LMWBABMTR, MRJVCGCWXVR, APMGNXMTR, MTN RCCJPRMEXVR; ICVMRLUAP MR MT XZAXGGXTJ RQBVBJ, MTN HTCYGXNWX, MTN UTNXVRJMTNBTW, BTJXVQVXJBTW CI NVXMLR, MTN RPCYBTW CI PMVN RXTJXTAXR, MTN NBRRCGDBTW CI NCUFJR, YXVX ICUTN BT JPX RMLX NMTBXG, YPCL JPX HBTW TMLXN FXGJXRPMOOMV; TCY GXJ NMTBXG FX AMGGXN, MTN PX YBGG RPCY JPX BTJXVQVXJMJBCT. JPX IBVRJ ACNXYCVN BR CJPXGGC.

第二关：恺撒移位密码

MHILY LZA ZBHL XBPZXBL MVYABUHL HWWPBZ JSHBKPBZ JHLJBZ
KPJABT HYJHUBT LZA ULBAYVU

第三关：同音替换密码

IXDVMUFXLFEEFXSOQXYQVXSQTUIXWF*FMXYQVFJ*FXEFQUQXJFPTUFX
MX*ISSFLQTUQXMXRPQEUMXUMTUIXYFSSFI*MXKFJP*FMXLQXTIEUVFX
EQTEFXSOQXLQ*XVFWMTQTUQXTITXKIJ*FMUQXTQJMVX*QEYQVFQTHMX
LFVQUVIXM*XEI*XLQ*XWITLIXEQTHGXJQTUQXSITEFLQVGUQX*GXKIE
UVGXEQWQTHGXDGUFXTITXDIEUQXGXKFKQVXSIWQXAVPUFXWGXYQVXEQ
JPFVXKFVUPUQXQXSGTIESQTHGX*FXWFQFXSIWYGJTFXDQSFIXEFXGJP
UFXSITXRPQEUGXIVGHFITXYFSSFI*CXC*XSCWWFTIXSOQXCXYQTCXYI
ESFCX*FXCKVQFXVFUQTPUFXQXKI*UCXTIEUVCXYIYYCXTQ*XWCUUFTI
XLQFXVQWFXDCSQWWIXC*FXC*XDI**QXKI*IXEQWYVQXCSRPFEUCTLIX
LC*X*CUIXWCTSFTIXUPUUQX*QXEUQ**QXJFCXLQX*C*UVIXYI*IXKQL
QCX*CXTIUUQXQX*XTIEUVIXUCTUIXACEEIXSOQXTITXEPVJQCXDPIVX
LQ*XWCVFTXEPI*IXSFTRPQXKI*UQXVCSSQEIXQXUCTUIXSCEEIX*IX*
PWQXQVZXLFXBIUUIXLZX*ZX*PTZXYIFXSOQXTUVZUFXQVZKZWXTQX*Z
*UIXYZEEIRPZTLIXTZYYZVKQXPTZXWITUZJTZXAVPTZXYQVX*ZXLFEU
ZTHZXQXYZVKQWFXZ*UZXUZTUIXRPZTUIXKQLPUZXTITXZKQZXZ*SPTZ
XTIFXSFXZ**QJVNWWIXQXUIEUIXUIVTIXFTXYFNTUIXSOQXLQX*NXTI
KNXUQVVNXPTXUPVAIXTNSRPQXQXYQVSIEEQXLQ*X*QJTIXF*XYVFWIX
SNTUIXUVQXKI*UQXF*XDQXJFVBVXSITXUPUUQX*BSRPQXBX*BXRPBVU
BX*QKBVX*BXYIYYBXFTXEPEIXQX*BXYVIVBXFVQXFTXJFPXSIWB*UVP
FXYFBSRPQFTDFTXSOQX*XWBVXDPXEIYVBXTIFXVFSOFPEIXX*BXYBVI
*BXFTXSILFSQXQXQRPBUIV

第四关:维热纳尔密码

K Q O W E F V J P U J U U N U K G L M E K J I N M W U X F Q M K J B
G W R L F N F G H U D W U U M B S V L P S N C M U E K Q C T E S W R
E E K O Y S S I W C T U A X Y O T A P X P L W P N T C G O J B G F Q
H T D W X I Z A Y G F F N S X C S E Y N C T S S P N T U J N Y T G G
W Z G R W U U N E J U U Q E A P Y M E K Q H U I D U X F P G U Y T S
M T F F S H N U O C Z G M R U W E Y T R G K M E E D C T V R E C F B
D J Q C U S W V B P N L G O Y L S K M T E F V J J T W W M F M W P N
M E M T M H R S P X F S S K F F S T N U O C Z G M D O E O Y E E K C
P J R G P M U R S K H F R S E I U E V G O Y C W X I Z A Y G O S A A
N Y D O E O Y J L W U N H A M E B F E L X Y V L W N O J N S I O F R
W U C C E S W K V I D G M U C G O C R U W G N M A A F F V N S I U D
E K Q H C E U C P F C M P V S U D G A V E M N Y M A M V L F M A O Y
F N T Q C U A F V F J N X K L N E I W C W O D C C U L W R I F T W G
M U S W O V M A T N Y B U H T C O C W F Y T N M G Y T Q M K B B N L
G F B T W O J F T W G N T E J K N E E D C L D H W T V B U V G F B I
J G Y Y I D G M V R D G M P L S W G J L A G O E E K J O F E K N Y N
O L R I V R W V U H E I W U U R W G M U T J C D B N K G M B I D G M
E E Y G U O T D G G Q E U J Y O T V G G B R U J Y S

第五关

109 182 6 11 88 214 74 77 153 177 109 195 76 37 188
166 188 73 109 158 15 208 42 5 217 78 209 147 9 81
80 169 109 22 96 169 3 29 214 215 9 198 77 112 8 30
117 124 86 96 73 177 50 161

第六关

OCOYFOLBVNPIASAKOPVYGESKOVMUFGUWMLNOOEDRNCFORSOCVMTUUTY
ERPFOLBVNPIASAKOPVIVKYEOCNKOCCARICVVLTSOCOYTRFDVCVOOUEG
KPVOOYVKTHZSCVMBTWTRHPNKLRCUEGMSLNVLZSCANSCKOPORMZCKIZU
SLCCVFDLVORTHZSCLEGUXMIFOLBIMVIVKIUAYVUUFVWVCCBOVOVPFRH
CACSFGEOLCKMOCGEUMOHUEBRLXRHEMHPBMPLTVOEDRNCFORSGISTHOG
ILCVAIOAMVZIRRLNIIWUSGEWSRHCAUGIMFORSKVZMGCLBCGDRNKCVCP
YUXLOKFYFOLBVCCKDOKUUHAVOCOCLCIUSYCRGUFHBEVKROICSVPFTUQ
UMKIGPECEMGCGPGGMOQUSYEFVGFHRALAUQOLEVKROEOKMUQIRXCCBCV
MAODCLANOYNKBMVSMVCNVROEDRNCGESKYSYSLUUXNKGEGMZGRSONLCV
AGEBGLBIMORDPROCKINANKVCNFOLBCEUMNKPTVKTCGEPHOKPDULXSUE
OPCLANOYNKVKBUOYODORSNXLCKMGLVCVGRMNOPOYOFOCVKOCVKVWOFC
LANYEFVUAVNRPNCWMIPORDGLOSHIMOCNMLCCVGRMNOPOYHXAIFOOUEP
GCHK

第七关

M C C M M C T R U O U U U R E P U C C T C T P C C C C U U P C M M P
R T C C R U P E C C M U U P C M P E P P U P U R U P P M E U P U C E
U U C U C C C M E M T U P E T P C M R C M C C U C C M P E C R T M R
U P M P M R C P M M C R U M C U U E U R P P C M O U U E U C C M U M
T U C U C U T M U U U P M U U C T C U P M M C C R P P P P M M M M E
E U M R C C C P U U E U P M U M M C C P E C U C U P C T C U E P M P
C U U E E U U U T P M M U C C T C C P P P C T P U C U C C C U R E U
T U C M E P C C E M U U U P R M M T M U C M M M C C C C C C M E P U
E C U M R E R U U U U M U R C C P M U U R U U P M U P R P P U U U U
M R C C P C P E U R M M M P U T C R U U E O U U U M C M U U R U P U
R U C M U C R U M M C U P U U M U C R E U U U P C C U R R C P R M C
T R C U U U R C T P P M U U C C U U U U M U U E P C R M E P M P U U
C C C U M M U U M C U C M C C C R T C C M E E U P T M U U M M M C C
P P T M C P T E O U U U M U U C R M C C C M C P R C R C E P M C M C
P U U C M C C O M T P R C M C P C P M C P C E R R E C C R R E C R U
P U E E P M U M T C U C E U U T P C E U M R C U U U R R U C R U U C
R P P T T C P C P C U C U M U M P E C E E R P M R M M U R U M E P M
R M M C P R U C R C P E E R P U U U U R E P C C M M E P P P R C C U
M P C C C M M E E U U P P E R U E C P U E M U C C U U C P U E P U C
M C M C U U C M M M C U P C C M M U U U C U O P U C U P M P U E C C
E U P M C E P R C T R M C C U U T E C E C C R M U C U R U C M U C R
C M P C C U O R U C T U C C M C U C M U M M T R U M C M M C P U U M
U P C C M P C U U E P C T E C T U U T C E E M T U C T E P P R U U M
U U E C M U M R U E P C U M P P O U R U C C U P U C U C U E P C M M
E C C U C E C P P C C C C O C R C R C R T U C P P T P U O C U O R U
C C C E U C P P M R R C E U U U R U R C C M T P P U R P P C T R R T
R U U P M T M U U E T R P R O E M P T P T E P R E R P T R U U U M T
R U M T P P P R U U P E O U T P T R O M U U E R M M E P U T T O T O
O M T P R M P P T M R E U R R U P M T R P P R E M U P R T R M M E O
U M M U P U U O U M E M O M E C P E U U U U C R U T T T R T U P T T
P E R E M U U R E E P E T R M P T R U U U O T R U U O O T T T O T T
E T E T O U P O M T U U O U T O E E T P T E M U U T U R C U O P T R
P O T E E M C O U U E P R M P T T T U P P R E T T R O E M U E T P O
P M T E R T E U U U P U P U U E M M O T O U M O R R C M U U U E T U

O T T E M T T C T M E T E R E U M U E E T U M E T P U T P U E T T M
P E E R T C P T O U U T R E R E T U T R E T R T R U T C M T C U U T
P O M T T P T P T O U M E O T T R P E P U T T T R T T O U M U U T P
E E C T M P P M U E C T R P U C T E U U E T P T O T P M T M C P U E
P P U P R M T P C R U R P R E M E R T U E E R O R O T O M M R C U U
E U T P T E P P E U U T P O T P P M E P E M T R E E U T U U T O T P
R E E R O P O R R M U U T M P R T T M E E E T E R U T M T O O C P E
P P M P M T P R R M E P R E U M M P R T R E E P U T T P E C T U R U
R C O P E E E O O U E M O M P T U E C E R M M M P P E P M U E M U R
T E U M R T T P U T C E R O E T M U U R O T U T T R M U E T E T T R
P R O U T U U P R E U T T R T P M T U P E E M E T E P T O E T U U T
E P T M U U E E P P T P M U P T E P R M U T T P M U M M E C R E T E
P T R T U R P M T O O U E E O T O U R U U R T U E U T P O M T P P U
R E O T C M C P R P R O O E E R U U E E R U M U U U C P P C P U E T
E R U R P O R P T P C T P E R E R M U T T R E U P R T M E C U R E P
P O U T M O T C T M P T P O E U U T O T P T O R E U E T U R M E T R
E P E E P R U C P E M M P T M U U T T E O E R M U R U U R U T P T T
E C E T O R T M T M E T T U E M U U C T O P E M U U E P U M C M U C
M T P O U C E C M T R E M C P C M C T P M M P P C M U U U U C M C C
C P T M M U C R E U U C T R R E U C U R E C P M R C E C U C E U C C
P M C T T P C R E U R M U T U P M P P M M C U T M C M C C E U U C T
U P U U U U U R C U M E P O T U U U C T E P C C P M C C T P C P U M
E R U C U M E M M R M U P C M U U C U C R U U U U C P C U P C E C M
C U U P O P C U U U U C U T T C P C M C U U C C E P U U P C M P U C
M M M P U U U E P M P P E C R C M P R E C R R U M C U E C P U P U C
E M P M U C R T U T U C R C C U P U U C U M M P U U U U E C U U C C
E C P P P R R M C M M E C C R M M R C C E C T U R M C E C C C P M M
M R P E C U U U C P P M M E C C M M R R C M U C M R C P C U C M U C
C C P C T R C U U E U C C M T E M C R C P E C C U U C U U C P E T P
C C P P T U M P C M P C M C E U C C C P C U C T C C C M T U M P T U
M E U C P P M U M P M M R E M C U M M M E R U C U C C M P U U E U C
P C E P P R U U C C U C T P U E T E R C M M M U R U U P U R P U E E
M U M U M R C U U C R M R C P T E M E C M M U C U C U U P P E T T T
M P C P M M U E M P P C U T P M C M U U P U C C P M P R C M C R P U
P M E M U U U R C O C P C U E P M R C P T M M M M C C E C U M C U U
C E C P P U C P M R M E P C U U R U C U C P R T U E R M C C R P M U

U R U U P M E U P C E C P T R U T U M C E C E P C U T C U C P E P C
C U U E T P P C P U U M C M M R O U C C P U C P P E P M E C R P C M
C U M P U C U U U E M M C U T M C U M C U E U C M U C C T P U R E U
P P C O P M P M U U M M M U U E T P U U U U U P P P P M U E C E R U
R P U R T P M P P P M E M C T U P C M E C P P C C E M U R M P T U U
R C U E P C U E C P U T C U R U C P R U M T C O C C M P U C M E P E
M P R U P P E C C P C U U C C C E U M R U U E U U E U C P C P M P U
C U M P U C U M P P R E U U U P E U P E U U C T P O T U P E T U O E
C O T T E M O T E U T E U M U P M U T P O U P E T E R P U T P R U U
U P O T T E P T R R M T C E T O R O P M T R E T R C O E T P R O E E
P T E P M M E U P E P E P U P U U R E E P E R T P E E C E P O R T U
E M E T T E P T E R M M T T E T T T P O R U M P T T E R P P U U R M
T T O M T M U M M U U T U O E P E U U O T C P E P T M R E R U R P E
T P P T T P C O R P T T T M U T R U P P T E R R E U R P R T R E T T
R C P R C U U M U P R U U U M T P R T R E T T U U U O C U M U U U U
M O T T P E M E T T E R P C T O E T U U R M E P E E O R C P E T M P
P R U T T R U U E T M O T M U U M T E R U T O T C R P M U R M U M R
M P M O O M O U O T P O R E M E M U P T O R T R R P O O U T P P P E
P M T P E O C T R R M E T O R T P E M M P E E E T R U U R U R P P U
P U R T R O U M T M R C U O T E T R C R P E E C P T E E U U E M T T
P U R U P E U O E U U M P E M U U T T E R E U M E R T T E T T T M E
U T M R T O R M E C U C U E U E P R U M T U U E R M U T R E U U P E
E M E E R C U U U T R M R T R M U U M M E P P T P R T E M T E M P E
U E T P O O O U U M O T O U T O O P E P R U U R T T T M U R T U T E
T P C O T E M T U O E T R M T E T E M M T U M O E E O O U M O P T P
R U T M R M T R T P T U U E P U U P U R R O E U E R U U O U P R T M
E T P E P P O T R M C M R U T T P U U E U R T T E E T E T U U E U E
E T U R R M E E M R E U R C T P E M U U R E P R U E O R U R U U P T
U M P E M T T P T U E M U P M O R T O O O U T P P M U U P U P E R E
R U U O U E E T U P E T E T P T T T E M R U U R T T T U T T M U P R
P R R U R U U T M T U R T C U E E O M R R T E T T M U T P P R P E P
T R E E O O T T E T R E T R U T P R U T M U U U T M U U C T U U P U
E R U E E M M U E E T T P E T M U M E T T E T T P M R E M R T P T E
T O U R T P P O E T T O M T P T E T E U T P U C U M U C U O E T U C
P E C U C M U P M U C U T T U C T U U M U C U R P U C P M C U U M U
C C E P C M M U C P T P U M U P U C M E C M P U M P P M U E M P P E

P U T E U M E P E P U P U U R M T P E M R P M M P T P O P R C R U E
P C M P P M R C C C P U C U P T U M U U P C P E M P T U U M C C C U
P C C U T U U U R C E M P E U C M R P P E P C C M M M U M P E C M T
R E R P U M P C C P T U C M C O P C U R U E C M T E C M M C C R P P
E P U U C U T M U U U C C T M C M E C P C U U U P U C U U U T C U C
C P T U U C C M M P P R E M C U U R U U M U E U U P P U C R P M R U
P C M U U E C U U C C U U R C E R R C U C P M P U U M T U U R C M P
E M U U U U C T U M T T T C U M P U M C M R T U U U C P P M E P U C
T O U P C M M C E C U M C P E C U P M T E P R U U R U R M P U P E R
C R U U C C C M P C U C M R M P M P E E P T P E M C U R C P C P U R
U T E U U E U U U P T C U C C C E M M T U T R E R E M P R R M U C C
R C U M U E P U P U E U E P M U T R U C C M U U C M M U U P M E C M
M E M U U U C M R P C M C U U C C E T P C P R R M U R R C T E C M C
M U U U U U U E C U U C U U T E P M U U R C C C U U R C U C E C P P
U C M U R C U U C R U C M C R C C C U C U M E M U U C P P P P R C R
U R U C M C P P C R M P U E P U M P O M U M M C U U U P C C C E C T
M R P U P M P O C C T P C M U U M C M C C T U C E C U U M C C M C U
E R T T R C M M U M T C P E R U U M M T R U E U M C M C C M C U U P
M U C C T P U M C U T P U M C U U U U C P P U C E T U P E R T R U U
U U M M C U M E E M C T C C P U R R U U R C P C U P C C U P M P M M
U R U U C C C E P R P U M M U T C M C M C C C U C P P C M E P C R E
M U U R C T P E M C M C C P R U C C U U U C C U U P C U U P U T R U
E E U U U E U C R P M R U U U O C P O C R P C M E C R C P C E C U U
E C P P U M P P E P C P R M P E U C P T U E M T U T T E O P R U E P
E P M T P U P T T R R E R P U E M M O P M U P R U U U M E M P P P U
T O U R O P R O P P M E T P R M T U U R P T P U U T O U U M T E P C
O E M C U U T P U U P T O T U U T T U U U R T P T R T T M O C T R U
T R O T T R O P T U M P P M U R T E U M T P E U M C M P R E P M R E
E E E U T T T E U U T M T P U R U E U U M T U P P U T T R E M T P T
R R U T U R T R U U T O T E R O T M U U U T M U P T P U U R T E R U
M M T M T T U P R P P P E M E P C M U M T R R E M U C E U P P T T T
T T P R U U U R T E E P U P U T M M T U P M R U O P E U E E T M M P
E M T P E C R E T M E O U T M E E P R E U M E M R T O T E M T O T P
T E C E P T U T R E E E M P P T P E E C P P T M U U T M U M P R M E
R E U U P T O E O P U E P T R T T E P M O U M P E U T M T T M U U U
T T P T E R M T R R U U R U U E U R T E E M U T T E P O U U E M E E

P C R U R M E T M E T O R E U U O T R T P R T T E U M M T P M M R P
E U U R E R T E O T U T R R O T O T E T T E O T U E U U E T U E T P
M U O O R T O U M C O T U E C E U U R E U U M T T E R U O T T M T E
T T E O T U T E P T R C T U U P P E R U T O U U E O R M U E M P R E
M U U P O P M O U O O T E C U O E T U C M T T P T T U U R T T M M O
P T P U C M T U U O M U M T T T O R T U P E T E T R O M T R E T T U
E U U T P P T M E U M U R U U U U R E T U T R U R R T T P P T T P O
E T E M U O T C O U E M T T M T U E U U P T U P U P T R O T U E E R
O E R O U E M C P T E R C P P T M U U M T O M C E M U T P T T T O U
T O E M T T P P C R E P O T E P P E R P O P P O T E U U U U R P U U
C P R P R M T R E U U E R M U C T O P T T U U T P M C T R M E T E M
M U O P T U U E T P P M M R M T U P R M U P R M O U P R T E U U U R
M M C O R T U M T O E T M U P M U T T P U T T E R M U U P C E T M T
U P T P P E T R U T T P O T M E C U R C P U O P M T P M C M P E P C
M M U O R R M P C M M O R C C U T C C O M C U U P R C P P P U C U U
E U P R U P M C E C T M C C U U R P P M U U E U U U U C E T U U R C
P U U R E U C E C U C C U E C U U U R C P P M C C C U P R M U C M U
C P R U P P U O M P U U U C M U U C P M U C R C P M M T C M M U O M
C M C C M U U P C C T U R U E U U U C U M T U C C M M U C T C R R U
R U M R P R U C U C E M U C C U U U E T U M C P C U R P U R C U U M
U P P C E M P P P U U M P P C C P R R C E C C R M C P P R C C R P P
M U U U R C M E P C P U C C C C U P R R U U P M C E M C U T M U C C
M E P M M P P M U U C C E M P R E U U T C P C U C M C C U C M R T P
M P C U C P P M R C M P C P E M P P P M R U U C C U U P R C E R T U
U P C U M U P U M P C R C C E P C U C C P M T R P C P C U U C R P P
R U R C C M E U U R U U M U R P E M R U C C M M U C R M C T M R P R
C U C M C U U C U M M U U U E M C T M C C M U C T C M U C M P M U T
R U R R E O C U C R C U P U C M P C E U C C E U U E P U M P T C C E
U R C U U C P U R C T P E U U M M U U U C C M M T U C R C R M R P O
U C U C U P C M P C U C T P M M U P U C U M U M C U T P P M E U U U
P U P C U U U U C M P U E M C U P C C R P P R U U M C C U C U P C P
C P C C U U U C U R C C P U R C U T U R E C R U U C M T C C C M U C
C P P P C M U C C U U U U U M M P U C R C U E C C T P C P M E E C M
U U C C C U U M C P C C C U U C U P C U P U T C M M C U M M M U M M
P U M M P T R M M P P P M R U U U C U U R E T U C P E C R P U R U R
C C C T P P M T P U P M P P M R M U R P U P U U U U U E P U C M P R

P P C C R O U U E C T U P C U P C C U U C P C P C M U E C M U T U U
P C U U T P P P C M M U P C C R U C E R T U C T E C M C U U E C R P
U M C U T C U E C C U P C U C C P U R P M M T U T P P O C U R C P C
P P M C M C C C P U P P M R U T E R M O T U M U U E M R C U U T P U
P P T T T M U O T T E R P R E T T R M T E M T E U U T T R P T T C U
T M T U P M R E U P M U E U U U U U P T E T C P U C E E C T E R M M
T M O T M P M E T R P E R O P E M E M M P R P T R U P T U O E U M P
P U R M U U E M M M P U C P U M U T M P E U U O P P U O M P T O T R
R M T P C P P P R E P E E R M R E M U T P O U E M P P E E R R M T R
T O M E P T E M U E P R T U R O O T O M U P P E R O T T P T T M P P
T P C U U U M T T U R E O P M T R E T T M E E U U O P M E R M P E T
E E R M U T T M M P E P O E T M E T E R U U O O R M E M M T R U U R
U O P R U P R P P U U U E E E T T T T P E U R E R R P U E T R U U E
O O O U E T E U U M U T U R U T R U U T O P O T U P M U R U U E R U
U U P U O O T T T P M E U E R T M O U M T P P P E O M T T U U U O E
U U E T U U E T U R P U M T M M E R R U U E T O T P T T T R P T M P
E E M T M E U U P O E T T P P P R U T E E C O U M E U U T T R T T T
R T T R T T M E P P T R T P O U T R T T O P E C R T P U T T C E M P
T O M R E T T T R E U C O T O T R P R U R P T U T E U U E P M E O T
M M U U U R R E T M O U M M P C P E T P T P R M T U P U E T E T E E
M C C T E R U R O E E P R R R R T P T U U M T P E E M C U O U U R E
C T U P P R T P P M T M U M C T T T P R R E O U T P E R U T M P U R
R U T U M O T T E E T M T R M R T O M T R R R T O P T T E R U O O M
U T P R M M P R P U E T M E U T T M P P R T P T P T T U U M R T E T
T R R O T U R U T R U U C M R C M T O C R U T P O T T P T M T E O R
R M R U E U R R T T O U R U P T U E C T E O T M T P R T P U M M R E
E E P O R P U R P R U M E M O T T R O P R U E T T U E T R O M T O U
E O P U T M T U R P T P R R T M O R E T C T M T M U E T T M R T T E
O R P C P P M M U M T T O U M T E U U R T R T R M E M U U T M T U T
R E T P M T P P M M

第八关

反射器		扰频器3		扰频器2		扰频器1		线路连接板	键盘
Y	A	B	A	E	A	A	A		A
R	B	D	B	K	B	J	B		B
U	C	F	C	M	C	D	C		C
H	D	H	D	F	D	K	D		D
Q	E	J	E	L	E	S	E		E
S	F	L	F	G	F	I	F		F
L	G	C	G	D	G	R	G		G
D	H	P	H	Q	H	U	H		H
P	I	R	I	V	I	X	I		I
X	J	T	J	Z	J	B	J		J
N	K	X	K	N	K	L	K		K
G	L	V	L	T	L	H	L	?	L
O	M	Z	M	O	M	W	M		M
K	N	N	N	W	N	T	N		N
M	O	Y	O	Y	O	M	O		O
I	P	E	P	H	P	C	P		P
E	Q	I	Q	X	Q	Q	Q		Q
B	R	W	R	U	R	G	R		R
F	S	G	S	S	S	Z	S		S
Z	T	A	T	P	T	N	T		T
C	U	K	U	A	U	P	U		U
W	V	M	V	I	V	Y	V		V
V	W	U	W	B	W	F	W		W
J	X	S	X	R	X	V	X		X
A	Y	Q	Y	C	Y	O	Y		Y
T	Z	O	Z	J	Z	E	Z		Z

K J Q P W C A I S R X W Q M A S E U P F O C Z O Q Z V G Z G W W
K Y E Z V T E M T P Z H V N O T K Z H R C C F Q L V R P C C W L
W P U Y O N F H O G D D M O J X G G B H W W U X N J E Z A X F U
M E Y S E C S M A Z F X N N A S S Z G W R B D D M A P G M R W T
G X X Z A X L B X C P H Z B O U Y V R R V F D K H X M Q O G Y L
Y Y C U W Q B T A D R L B O Z K Y X Q P W U U A F M I Z T C E A
X B C R E D H Z J D O P S Q T N L I H I Q H N M J Z U H S M V A
H H Q J L I J R R X Q Z N F K H U I I N Z P M P A F L H Y O N M
R M D A D F O X T Y O P E W E J G E C A N P Y F V M C I X A Q D
Y I A G Z X L D T F J W J Q Z M G B S N E R M I P C K P O V L T
H Z O T U X Q L R S R Z N Q L D H X H L G H Y D N Z K V B F D M
X R Z B R O M D P R U X H M F S H J

密钥

```
07161504130201l0
```

字母

```
begin 644 DEBUGGER.BIN
(-&>`_EU-_/$`

end
```

第九关

```
begin 600 text.d
MM5P7)_8F_,H[JOF1C//L/W+)%QSK*Q37CJ-N 'W[_;CQSTW'UY0S2,\LQVG0
M@1&HY^1MHYI\>2P'F:6Y*E%X4A&$2'=L28$$..9[*-ZIGA_VP(GIPK[CW3^L
M55+6OD^&=FS61(L96YG>  '59*1Q^)/C?$1/C&9PN35-HP;.>V8_/P(.:+R(
M61]'NG^UP:,#57MMQSKN[N7M>1NE;2(!RUA495Q16!;Q<*(*[C**A*@%A+=S
M8AR45+G$-#8A?29V_.6%7*6D$J_G4JX'JM^1? K@._#(B/N7-<YNU;/,JF8C
M6LD[90MVJ2'I*.G@>9U%!E(33!S^K# N7JH_Y5RYE&=J@S!>^<C3Y=PD%-RP
M9&++^*JLPOK%T)-5KI>IUA*W;7;&D(D-2/U'$3\C7 ?]B* 3*C/Y!%U >&V6
M%W85NJ:JPO(>#C1)CPEL&^H3YKR2.59XJVD??\MX+ [S?3X_F^/*1$NGH$B&
MI$L2-C'E/@OD*&5;6+P+G1S D49AO=#9\C!4D$/F;C(H#MX:\%G[K[OR+2RG
M@@SCSVG!A5%FEV!=$YD*V.2T06@>C-&)3H<:Y9BOR=V#S_>\:S8GZ.*A*$!T
MZOE=/4QWLLB<[:K8T TZ@C9_,( #D:/G4)P2>,S?%9: Q]MV0;?F9;F1VP'@
M=!XCI_M>2?F=' ;20):%Y61[.! -W8%7M3BJUX/&!-E@A7C\(>5SZXESA$LZ
MF\_U//JGV*KKHE2599279628P-9J!*J@ DPJF]M2/>DXHA?JT*^2C7;_-9B;
MBM'CFTYUR#DOA7.J4ZW8=+3(9O>#4A+^!=4IV_6A!(PNGZ:T$O)659KNGS=>
MN*?LQ3$6F*I43Q(3_U:64V/L9$<E%*>*#A9P>@(66#XDS!)-'*\JZE.,=G29
MOJLH!9.Y#+=?]!*C?2/?H5O!A]<KW^H%J *&>+EXK;II6)N6JY$%UB'BN3'F
MMS[XKP#JY(:30V);U2,5PG 6$!46;.B/K'E7$4'MKN1]* YX^R*Q?Q+;,*./
MPL((>]UF90L7[<]9^E0*:NMBI(Q+B'>-IHF+,J0&*G0F.5L8@*_)<Y$<ZRU=
M']&L9!ND1Y<V[D:/;4J(+#X(NIKKDFO@#:5O_3G%7]AG5H.? ,%;D)=7'HKE
M.(_E=(*(W5HO3RA5WP8<!ZM.K2T.:&#P\LV;!7W$ K3)/A7D&P8SVO3-?$U1
M2J10K3T>2)OVRA'Y;C<DZVV+'$VXI_ $JZ^)39,'.7MK,0*QOP9O6QRQ0F(*
M&8J9O!Z*>N;S%MD%%A.SD?'^\K]*R_@XE6V# >&P.$L#$,%N*C[H:A_EPH$V
M\H)(;C0#3^C] T9Z0=,9UQ(3N^3D],9PVM<AJ.T:('(.=1FB;NBV_YS!\7ON
M?-T%5B;2J^TORBWA^Z$B'$K8LC;'A+>@87(6!8Q%PRS=^;Y*0$PC*>;I!NI*
@#%0SNY_0_-EK1>;84QMT0/(KQQ2LL+R##K:I=NK7.OT

end
```

第十关

短信息:

10052 30973 22295 13534 12990 66921 15454 81904 58209 26472 18119
11542 99190 01294 87266 20201 55809 80932 92390 96710 64341 91354
27685 27572 48495 78859 80627 33369 29356 36094 85523

长信息:


```
begin 600 text.d
M.4#)>S I:R!!4)NA+\%T%V/(AW!7HHDPS$;T[\E!RWA?,J8:X#D[!:XF,A>K
MXT9$Q)37\IOMG6KL-$6?A!#FZ2Y)N+4%*.^2K!SP?Z2'8O7LZ}QP \T=QG-*
MAMJA;Q@3H(8^U/L<ILL%TA0J9M*F@8F?H:76%<33JOESAP=@3:(\:8NBGFM0
M,MP3B^CP%/D8DICZ$VO(7IS(DTJRZ&#Y- 7I\-#VI0">J@+O!CT.+6B9K$J%
4:EAB9%1@;(P+I>1!#<+2+;(7.W<

end
```

15000美元大奖
挑战智力极限

你若能将本书所附10道密码按其规则破译，

即可获得15000美元巨奖。领奖方式详见内文。

辛格能够把令人害怕的数学世界说得和小孩游戏一样简单，这能够吸引许多有数学恐惧症的读者。

——每日电讯

本书讲述了从密码怎样创建到它们怎样被破解的故事，以及围绕它们而产生的种种诡计。

——纽约时报



ISBN 7-5443-0218-0/N·1
定价：20.00元

[General Information]
书名=密码故事　人类智力的另类较量
作者=[英]辛格（Singh，S.）著
页数=364
SS号=10406094
出版日期=